T.C.
KADİR HAS ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
FİNANS ve BANKACILIK DOKTORA PROGRAMI

BANKALARDA OPERASYONEL RİSK YÖNETİMİ VE BİR ENDEKS ÖNERİSİ: ORYOS ENDEKSİ

Doktora Tezi

HASAN AYKIN

İstanbul, 2009

T.C.
KADİR HAS ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
FİNANS ve BANKACILIK DOKTORA PROGRAMI

BANKALARDA OPERASYONEL RİSK YÖNETİMİ VE BİR ENDEKS ÖNERİSİ: ORYOS ENDEKSİ

Doktora Tezi

HASAN AYKIN

Danışman: DOÇ.DR. M.HASAN EKEN

İstanbul, 2009

GENEL BİLGİLER

İsim ve Soyadı	**:** Hasan AYKIN
Programı	**:** Finans ve Bankacılık
Anabilim Dalı	**:** Sosyal Bilimler Enstitüsü
Tez Danışmanı	**:** Doç Dr. M. Hasan EKEN
Tez Türü ve Tarihi	**:** Doktora - Temmuz 2009
Anahtar Kelimeler	**:** Operasyonel Risk Yönetimi, Basel, Olgunluk Modeli

ÖZET

BANKALARDA OPERASYONEL RİSK YÖNETİMİ VE BİR ENDEKS ÖNERİSİ:ORYOS ENDEKSİ

Ekonominin istikrarlı olarak büyümesi ve kalkınmanın sağlanması sağlıklı işleyen bir mali sistem alt yapısıyla yakından ilgilidir. Bu alt yapının önemli aktörleri düşünüldüğünde ilk sırada kuşkusuz, fon fazlası olanlarla fon açığı olanlar arasında köprü vazifesi gören bu transfere aracılık eden, finansal sistemin lokomotifi bankalar yer almaktadır. Üstlendiği önemli ve hassas görev nedeniyle bu kurumların etkin bir risk yönetim sistemine sahip olmaları gerekmektedir.

*Bu çalışmada, finansal kurumlarca önemi son yıllarda daha iyi anlaşılan ve gittikçe daha da artan operasyonel riskin yönetimi ele alınmış olup, sayısallaştırılması diğer riskler gibi kolay olmayan bu riskler için olgunluk modeli kullanılarak bankalar için "**O**perasyonel **R**isk **Y**önetimi **O**lgunluk **S**eviyesi" (ORYOS) endeksi hesaplanmıştır.*

Çalışmanın amacı iki noktada toplanmaktadır; bunlardan ilki, hesaplanan bu endeksle bankaların hem kendi hem de sektördeki seviyelerini daha iyi görebilmeleri, eksik noktalarını tespit edip kendilerine hedefler belirleyebilmeleridir. İkinci amaç ise bu endekse bağlı olarak belirlenecek "ORYOS Sermaye Yükümlülük Çarpanı" ile bankaların sermaye yeterlilik standart oranının hesabında bir düzeltme katsayısı olarak bankanın operasyonel risk yönetimi olgunluk seviyesinin dikkate alınmasını sağlayarak temel gösterge, standart yaklaşım ve alternatif standart yaklaşım kullanılarak yapılan sermaye yeterlilik hesabında daha gerçekçi bir ölçüm ortaya koymaktır.

GENERAL KNOWLEDGE

Name&Surname	**:** Hasan AYKIN
Graduate Programme	**:** Ph.D. in Finance and Banking
Institute	**:** Graduate Institute of Social Sciences&Humanities
Supervisor	**:** Asst. Prof. M. Hasan EKEN, Ph.D.
Degree Awarded & Date	**:** Ph.D. - July 2009
Keywords	**:** Operational Risk Management, Basel, Maturity Model

ABSTRACT

OPERATIONAL RISK MANAGEMENT IN BANKING AND PROPOSAL OF AN INDEX: ORMML INDEX

Stability in economic growth and development is highly correlated to an efficient and sustainable financial sector. The most crucial agent of this relationship is surely the banks acting as the engine of financial system by intermediating, like a bridge, funds between surplus and deficit agents. Thanks to their pivotal and delicate role, banks are required to have an effective risk management system.

The dissertation covers both management of operational risk which has been gradually given more importance by financial institutions and also evaluation of an index for banks called "Operational Risk Management Maturity Level" (ORMML) Index for those risks whose quantification is more difficult compared to other types.

The study has two main purposes to achieve: the first is that banks could benchmark their own operational risk management level against those of industry thereby strengthening their weaknesses. The second is to propose a much more realistic recalculation of capital adequacy standard ratio in basic indicator, standard indicator and alternative standard indicator approaches by incorporating a fine-tuning factor into the equation called "ORMML Capital Requirement Multiplier" derived from the ORMML Index.

ÖNSÖZ

İnsanların mutlu, huzurlu ve refah içerisinde yaşayabilmesinin ön koşulları arasında ekonomik istikrarın sağlanması olduğu şüphesizdir ki bunun sağlanması da kuşkusuz istikrarlı ve sağlam bir finansal sektörün tesisinden geçmektedir. Bu bağlamda, istikrarın yakalanması ve sürdürülebilir olması, varlıklardaki veya süreçlerdeki açıklıkların bir tehdit tarafından kullanılması, zarara uğratılması ihtimalini azaltmakla ya da ortadan kaldırmakla, yani diğer bir deyişle etkin bir "Risk Yönetimi" ile olasıdır.

2008 yılının son çeyreğinde ABD konut sektöründe yaşanan finansal sorunlar dalga dalga büyüyerek başta gelişmiş ekonomiler olmak üzere hemen hemen dünyanın her ekonomisini önemli derecede etkisi altına almış; uzun yıllardır görülmeyen ölçekte bir durgunluğun yaşanmasına sebebiyet vermiştir. Uluslararası arenada yaşanan ve etkileri derin ve belirsiz gelişmeler ışığında özellikle hazine işlemleri, seküritizasyon, bilanço dışı yükümlülükler ve likidite riski açılarından Basel II uzlaşısının yeterliliği tartışılır hale gelmiş olup, eksikliklerinin yeniden gözden geçirilmesi doğrultusunda çalışmaların devam ettiği bilinmektedir.

Yaşanan bu küresel krizde bile, özellikle kurumların daha fazla kar elde etme saikiyle risk tolerans seviyelerindeki artışlara istinaden daha fazla kredi verme ve işlem yapma güdüleri, türev piyasalarının giderek karmaşıklaşan yapısı gibi etkenlerde operasyonel riskin izlerine rastlamak mümkündür. Dolayısıyla operasyonel risk diğer risklere nazaran ölçümü ve yönetimiyle daha karmaşık bir risk türü olup yaratacağı etkilerle de önceden tahmin edilemeyecek boyutlarda kayıplara yol açabilmektedir. Bu yüzden bankaların operasyonel riske esas tutar için ayırmaları gereken sermayenin daha hassas ve içerisinde bankanın operasyonel risk yönetim seviyesini dikkate alan bir yapıda hesaplanması önerilmektedir. Operasyonel riskin ölçülmesine yönelik olarak Basel komitesinin bankalar için önerdiği temel gösterge, standart yaklaşım ve alternatif standart yaklaşımın üçünde de bankanın elde ettiği yıllık brüt gelir ve kredi hacmi tutarları gösterge olarak dikkate alınmakta olup bankanın mevcut operasyonel risk yönetim uygulamaları gözardı edilmektedir.

Bu doğrultuda çalışmanın temel amacı; operasyonel risk yönetimine ilişkin bir endeks önerisi (ORYOS Endeksi) getirerek bu endeksten türetilecek sermaye yükümlülük çarpanının sermaye yeterlilik hesabında kullanılmasını ve böylece bankaların operasyonel risk yönetimi olgunluk seviyelerinin söz konusu hesaplamada dikkate alınmasını sağlayarak operasyonel risk yönetimi için daha gerçekçi bir yaklaşım elde etmek ve bankaların faaliyet ve sahiplik türleri açısından sektördeki yerlerini görmelerine olanak sağlayarak diğer bankalarla karşılaştırma yapabilmelerine imkan sağlamaktır.

Geçen yıl aramızdan ayrılan sevgili hocam ve ilk danışmanım Prof. Dr. İlhan Uludağ'ı rahmetle anarak, çalışmanın tamamlanması sürecinde görüş ve yorumlarıyla katkıda bulunan danışman hocam Doç. Dr. M. Hasan Eken'e, Takasbank'ta aynı birimi paylaştığım Mustafa Demir ve Sema Sarıkuş'a, Marmara Üniversitesinden Gamze Alev, Sinem Kangallı ve Gülşah Çolakoğlu'na ve anket çalışmasının oluşmasında emeği geçen sermaye ve para piyasalarındaki tüm çalışma arkadaşlarıma teşekkürü bir borç bilirim.

Eğitim hayatım boyunca büyük fedakarlıklarla beni destekleyen ve dualarını benden esirgemeyen sevgili annem Saniye Aykın ve rahmetli babam Ali Aykın'a, bu zorlu süreçte göstermiş olduğu anlayışla bana destek ve moral veren eşim Songül Aykın'a, çocuklarım Ali Can ile Anıl'a ve ailemin diğer tüm fertlerine sonsuz teşekkür eder, çalışmamın tüm ilgili kişi, kurum ve kuruluşlara yararlı olmasını temenni ederim.

İstanbul, 2009 Hasan AYKIN

İÇİNDEKİLER

Sayfa No.

TABLO LİSTESİ

Sayfa No.

ŞEKİL LİSTESİ

Sayfa No.

GRAFİK LİSTESİ

Sayfa No.

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AHP	Analytic Hierarchy Process
AHS	Analitik Hiyerarşi Süreci
AICPA	American Institute of Certified Public Accountants
AKG	Anahtar Kontrol Göstergesi
APG	Anahtar Performans Göstergesi
ARG	Anahtar Risk Göstergesi
AS/NZS	Australia and New Zealand Standards
BCBS	Basel Committee on Banking Supervision
BDDK	Bankacılık Düzenleme ve Denetleme Kurulu
BGYS	Bilgi Güvenliği Yönetim Sistemi
BIS	Bank for International Settlement
Bkz.	Bakınız
BS	British Standards
BT	Bilgi Teknolojileri
CAN/CSA	Canadian Standards Association
CMM	Capability Mature Model
COBIT	Control Objectives for Information and Related Technology
COSO	The Committee of Sponsoring Organisations of the Treadway Commission
EC	European Commission
Ed.	Editör
EFT	Elektronik Fon Transferi

ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
FED	Federal Reserve Bank
FSA	Financial Services Authority
G-10	Group of Ten
G-30	Group of Thirty
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IR	Inherent Risk
ISACA	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information Technology
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
İÖY	İleri Ölçüm Yaklaşımı
JIS	Japanese Standards Association
K	Kurtosis
KCI	Key Control Indicator
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KRY	Kurumsal Risk Yönetimi
LAN	Local Area Network
OECD	Organisation for Economic Co-operation and Development
ORY	Operasyonel Risk Yönetimi

ORYOS	Operasyonel Risk Yönetimi Olgunluk Seviyesi
PUKÖ	Planla - Uygula -Kontrol et - Önlem al
RMD	Riske Maruz Değer
RMI	Risk Management Index
RR	Residual Risk
RYE	Risk Yönetim Endeksi
s.	sayfa
SEC	US Securities and Exchange Commission
SEI	Software Engineering Institute
SOx	Sarbanes Oxley Kanunu
SPK	Sermaye Piyasası Kurulu
SPSS	Statistical Package for the Social Sciences
TBB	Türkiye Bankalar Birliği
TCMB	Türkiye Cumhuriyet Merkez Bankası
TKY	Toplam Kalite Yönetimi
TÖAİK	Tanımla, Ölç, Analiz Et, İyileştir ve Kontrol Et,
VaR	Value at Risk
VPN	Virtual Private Network
WAN	Wide Area Network

GİRİŞ

Risk yönetimi, doğuşu ve gelişimi itibariyle 1970'li yıllardan sonraki dönemi kapsayan ve bu dönemdeki pazar ekonomilerinin evrimini etkileyen bir süreçtir. Finansal piyasalarda bilinen riskler 1990'lı yıllara kadar kredi ve piyasa riskleri olarak ifade edilmekteydi. Ancak daha sonraları finansal kurumların pozisyon almaya bağlı olmayan bir takım risklerle de karşı karşıya olduklarının anlaşılması ve özellikle de daha sonradan operasyonel risk olarak tanımlanan ve kurumlara mali ve repütasyonel olarak ciddi kayıplar veren unsurların ön plana çıkmasıyla düzenleyici otoriteler de konuya daha fazla eğilmeye başlamışlardır. Kurumlarda önemli miktarlarda kayba yol açan gelişmelerin kredi veya piyasa riski ile doğrudan bağlantılı olmamalarından dolayı, önemli miktarda kayıplara yol açan nedenlerin olayların ortaya çıkmasının önleyecek mekanizmaların bulunmaması, bulunsa bile etkin çalışmaması ya da konunun yeterince dikkate alınmaması olduğu düşünülmektedir. 1990'lı yılların sonlarından itibaren operasyonel risk kavramı düzenleyici otoriteler için giderek daha fazla önem verilen ve yakından izlenmesi, gözlenmesi ve ölçülmesi gereken bir risk unsuru olarak karşımıza çıkmış ve risk yönetimi kapsamına alınmıştır.

Finansal sektörde yaşanan artan otomasyon ve çok hızlı teknolojik değişimler, sunulan ürün ve hizmetlerdeki çeşitlenmeler neticesinde yeni finansal ürünlerin daha karmaşık yapıya bürünmeleri gibi etkenler operasyonel risk kavramının finansal kurumlar üzerindeki etkisinin artmasına sebep olmuştur. Dünya genelinde yaşanan küreselleşme finansal piyasaların tanımını ve bu piyasalarda işlem yapma düşüncesini değiştirmiştir. Küreselleşmeye bağlı olarak finansal kuruluşların dünyanın çeşitli bölgelerinde hizmet verir hale gelmeleri, operasyonların yakından takip edilmesi olanağını azaltmıştır. Gelişmekte olan piyasaların hızlı yükselişi, finansal kuruluşların merkeze uzak ofislerinin değişik müşterilere standart olmayan hizmetler vermelerini zorunlu kılmıştır. Sınır ötesi yatırımlar artmış, takas, saklama ve ödeme hizmetleri merkezileşmiştir. Bilgi sistemlerindeki gelişim ve iletişim maliyetlerindeki düşüş finansal işlemlerin elektronik ortamlarda gerçekleşmesine neden olmuştur. Yeni ürün ve hizmetler, özellikle türev ürünler riskleri artırıcı bir diğer faktör olmuştur. Başlangıçta risklere karşı korunma amacıyla kullanılan türev ürünlerdeki gelişmeler risk yönetim sürecini çok yönlü ve karmaşık hale getirmiş, daha karmaşık hizmet ve ürünler ise operasyonel risklerin artmasına neden olmuştur. Yeni ürün ve

hizmetlerle birlikte işlem hacimlerindeki değişkenlikler artmış, bu nedenle işlem hacimlerinin yapısını ve bunun kuruluşun faaliyetleri üzerindeki etkisini anlamak operasyonel risklere karşı etkin bir kaynak dağılımı sağlamak açısından vazgeçilmez hale gelmiştir. Öte yandan, bilgi teknolojilerindeki gelişmeler işlem hızını ve iletişim olanaklarını artırarak finansal kuruluşlar için yeni sistemlerin ve bilgisayar donanımlarının geliştirilmesini zorunlu kılmıştır. Normalde daha fazla hız ve daha az insan hatası anlamına gelen bu sistemler aynı zamanda, sistemlerin aksaması ya da yaşanan değişimlere kolaylıkla uyum sağlayamaması halinde ortaya çıkabilecek risklerin de artmasına neden olmuştur. Ayrıca, bölgesel ya da global krizler, doğal afetler, terörist saldırılar, yasal düzenlemelerdeki değişimler gibi piyasalardaki beklenmeyen olayların finansal kuruşlar üzerinde yıkıcı etkiler yaratabilme potansiyeli, operasyonel risklere bakış açısını değiştirmiştir.

Günümüzde finansal piyasalar gittikçe daha rekabetçi bir ortama girmekte ve risk yönetimi de finansal kurumların faaliyetlerinin kalbi olmaya devam etmektedir. Risk yönetimi önceleri finansal faaliyetin bir parçası olarak algılanmayan, henüz emekleme döneminde olan sadece işler kötü gittiğinde alınacak tedbirlerin neler olması gerektiğini belirlemeye yarayan bir araç veya bir yöntemdi. Son yıllardaki yönetimsel uygulamalar bakımından finansal kurumlarda kurumsal risk yönetiminin önemi artmış ve dolayısıyla kurumsal faaliyetlerin stratejik analizi yapılmaya başlanmıştır.

Bu gelişmelere paralel olarak gelişmiş ülkelerin merkez bankaları ile düzenleyici, denetleyici otoritelerin yöneticileri tarafından oluşturulmuş olan Basel Komitesi bankacılık sektörünün istikrarlı, güvenilir ve sağlam bir şekilde faaliyetlerini sürdürebilmesini teminen ortak çalışmalar yürütmeye başlamıştır. Komitenin çalışmaları ve ürettiği tavsiye kararları sektörel düzenlemelerin kalitesinin artırılmasını amaçlamış ve zamanla Komite kararları dünyadaki önemli bankacılık otoriteleri tarafından uygulanmaya başlanmıştır. Ülkemizde de Komitenin önerdiği özellikle bankaların maruz kaldıkları risklere karşı güçlü ve istikrarlı bir şekilde faaliyetlerini sürdürebilmelerini teminen sermaye yeterliliğinin tesis edilmesine ilişkin kararları BDDK tarafından ülkemiz bankacılık sektörünün özgünlüğü çerçevesinde yasal mevzuat haline getirilmiştir.

Bankalarda operasyonel risk yönetimi kapsamında neler yapılması gerektiğini ve bankalarımızın gelinen süreçte bu konuda hangi seviyede olduklarını açıklamaya çalışan bu çalışma dört temel bölümden oluşmaktadır. Birinci bölümde genel olarak riskin tanımı, tarihçesi, operasyonel risk kavramı kısaca açıklandıktan sonra operasyonel riskin yönetilmesine ilişkin ulusal ve uluslararası kurumlar tarafından oluşturulmuş mevzuat ve tavsiye kararlarından bahsedilerek operasyonel risk yönetiminin, unsurları ve araçları açıklanmaktadır.

Çalışmanın ikinci bölümde risk yönetimine ve bilgi sistemleri risk yönetimine ilişkin olarak geliştirilmiş olan ve genel kabul gören standartların yaklaşım metodolojileri ve içerikleri açıklanmış olup ilerleyen kısımda operasyonel riskin temel unsurlarını oluşturan insan, sistem, süreç ve dışsal faktörlerden kaynaklanan risklerin daha etkin bir şekilde nasıl yönetebileceğine ilişkin temel yaklaşımlar anlatılmıştır.

Üçüncü bölümde çalışmanın uygulama kısmına esas teşkil eden olgunluk modeli yaklaşımı ve oluşturulan endeksin alt faktörleri arasındaki göreceli ağırlıklandırmanın yapılmasında kullanılan Analitik hiyerarşi süreci ve “Operasyonel Risk Yönetimi Olgunluk Seviyesi” (ORYOS) endeksinin hesaplanma yaklaşımı açıklanmıştır.

Çalışmanın dördüncü bölümünde ise çalışmada kullanılan anketin hazırlanma süreci, ilgili kurumlara gönderilmesi ve geri dönüşler sonrasında elde edilen sonuçların bankaların sahiplik ve faaliyet türü açısından değerlendirmesi; anketin sonuçlarının istatistiksel olarak güvenilirlik, korelasyon, varyans ve kümeleme analizleri anlatılarak anket sonuçlarına göre sahiplik ve faaliyet açısından gruplanan bankaların ve sektörün ORYOS endeks puanları hesaplanarak sektörün ve banka gruplarının operasyonel risk yönetim seviyeleri grafiklerle değerlendirilmiştir. Ayrıca geliştirilen ORYOS endeksine bağlı olarak belirlenen ORYOS sermaye yükümlülük çarpanı ile de, sermaye yeterliliği standart oranında hesaplanan “Operasyonel Riske Esas Tutar” içinde bu çarpanın bir düzeltme katsayısı olarak kullanılması düzenleyici otoriteye önerilmiştir.

Çalışmanın sonuç bölümünde ara bölümler kısaca özetlendikten sonra genel bir değerlendirme yapılmıştır.

BİRİNCİ BÖLÜM

1. RİSK KAVRAMI, OPERASYONEL RİSKİN UNSURLARI VE ÖLÇÜMÜ

1.1. Risk Yönetimi

Bu bölümde risk ve risk yönetiminin tanımı yapılıp, risk yönetiminin tarihçesi ve amaçları açıklandıktan sonra bankacılık sektöründeki temel riskler: kredi riski, piyasa riski ve operasyonel risk hakkında bilgi verilecektir.

1.1.1. Risk Yönetiminin Tanımı, Amacı ve Tarihçesi

Risk sözcüğünün kökeni ya Arapça rızık/rısk (risq) ya da Latince riziko (risicum) sözcüklerinden çıkmıştır[1]. Gerek İngilizce'de gerekse Türkçe'de risk (ya da riziko); kayıp, hasar tehlikesi, ya da kayıp, hasar tehlikesi olasılığı, sigorta edilen şey ya da kimse olarak tanımlanmaktadır[2].

Finansal risk parasal bir kayba maruz kalma olasılığıdır. Finansal risk de beklentilerdeki farklılığa ve deneyime bağlı olarak kişiden kişiye, kurumdan kuruma farklılık göstermektedir.[3]

Bankalar, tasarruf sahiplerinin kısa vadeli ve likit olan fon arzları ile fon talep edenlerin uzun vadeli ihtiyaçları arasındaki uyumsuzluğu gidermek suretiyle vade ayarlaması; tasarruf sahiplerinin küçük arzları ile fon talep edenlerin büyük ihtiyaçlarını dengelemek suretiyle miktar ayarlaması yapan, risk azaltıcı ve dağıtıcı yönde faaliyet gösteren ve ödemeler sisteminin çalışmasını sağlayarak ekonomi için çok önemli katkıları olan finansal aracılardır[4].

---

[1] Jake Ansell ve Frank Wharton, **Risk: Analysis, Assessment and Management**, John Wiley and Sons, 1992, s.4-5'den Arman T.Tevfik, **Risk Analizine Giriş**, 1.Baskı, İstanbul: Alfa Basım Yayım Dağıtım, 1997, s.1.
[2] Arman Tevfik, **Risk Analizine Giriş,** 1.Baskı, İstanbul: Alfa Basım Yayım Dağıtım, 1997, s.1.
[3] Ünal Bozkurt ve Diğerleri, **İşletme Finansının Temelleri**, İstanbul: Literatür Yayıncılık, Ekim 1997, s.251'den Engin Kurun, **Faiz Riski Yönetimi ve Türkiye Uygulaması**, 1.Baskı, Sermaye Piyasası Kurulu, yayın no:181, Ankara:2005, s.3.
[4] İlhan Uludağ ve Erişah Arıcan, **Finansal Piyasalar Ekonomisi (Piyasalar-Kurumlar-Araçlar)**, İstanbul:Beta Yayınları, 1999, s.117.

Risk yönetiminin amacı bankacılık açısından düşünüldüğünde; bankacılığın, maruz kalınan risklerin, bankanın sağlıklı, güvenli ve karlı bir işletme olarak varlığını sürdürebilmesi amacıyla yönetilmesi esası üzerine kurulu bir yapı olduğu söylenebilir.[5]

Karlılığa ve likiditeye ilişkin kararlar daima belirsizlik koşulu altında alınır ve bu belirsizliği gidermek üzere de tahminde bulunulur. Tahmin ile gerçekleşmenin aynı ölçülerde olmaması veya yapılan tahmindeki hata bir kayıp yaratıyorsa, bu riskin kendisidir. Özellikle bankalarda yanlış tahminlere dayanarak alınan kararlar, sadece bankaların karlılığı için değil bankanın likiditesi için de risk yaratırlar. Bankanın karlı olduğu halde ödemeleri zamanında yapamaması veya ödemeleri zamanında yapabilmesine rağmen ortaklarını memnun etmeyen bir karlılık düzeyi bankanın geleceğini tehdit eden en temel riskin kaynağını oluşturmaktadır.[6]

Günümüzdeki anlamına yakın bir şekilde "Risk Yönetimi" kavramının uygulanmaya başlanması, şirket içinde işinin sadece risklerin takibi ve yönetiminden sorumlu olması gereken bir kişinin istihdam edilmesinin gerektiği gibi düşünceler 1950'lerden sonra şekillenmeye başlamıştır[7]. Ama finansal risk yönetimi konusunda yapılan akademik çalışmalar ve sektörün konuya olan ilgisi özelikle 1950'lerde Harry Markowitz'in önemli çalışmaları sonrasında özellikle artmıştır. Markowitz esas olarak o güne kadar portföy yönetimine dönük geliştirilen düşüncelerin çoğunlukla geleceğe dönük tahminler içermesine rağmen risk kavramına hiç değinmediğinden hareketle optimal portföy oluşturma tekniklerini formüle etmiştir. Markowitz esas olarak tüm yumurtaların aynı sepete konulmaması gerektiğini, çeşitliliğin iş sahibi veya yatırımcı açısından daha güvenli bir ortam oluşturduğunu söylemiştir[8].

1980'lerden sonra ise "risk yönetimi" kavramına olan ilginin artmasında özellikle makro düzeyde gerçekleşen üç unsur önemli bir rol almıştır: piyasalarda yaşanan ve giderek daha fazla artan oynaklık (volatilite), sermaye piyasası işlemlerinde oluşan önemli

[5] Hasan Candan ve Alper Özün, **Bankalarda Risk Yönetimi ve Basel II**, 1.Baskı, İstanbul:T.İş Bankası Kültür Yayınları, 2006, s.5.
[6] Hasan Kaval, **Bankalarda Risk Yönetimi,** Ankara:Yaklaşım Yayınları, 2004, s.23-24.
[7] R.B. Gallagher, "Risk Management: New Phase of Cost Control", **Harvard Business Review**, (Sep-Oct. 1956)'den Imad A. Moosa, **Operational Risk Management**, Eeastbourne:Palgrave Macmillan, 2007, s.77-78.
[8] Şenol Babuşçu, **Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi**, Ankara: Akademi Consulting&Training, Eylül 2005, s.6-7.

miktardaki hacim ve adet artışı ve son olarak da bilgi teknolojilerinde gerçekleşmiş olan olağanüstü ilerlemelerdir. 1990'lardan günümüze kadar olan süreçte özellikle de gelişmekte olan piyasalarda yaşanan ekonomik krizler sermaye piyasalarında önemli fiyat ve endeks oynaklılarına sebep olmuştur. Artan piyasa oynaklılarının yanında yeni alternatif yatırım araçlarının icat edilmesi ve dünya genelinde yaygınlaşan kısıtlamaların kalkması (deregülasyonlar) neticesinde ürün çeşitliliği artmış, ürün yapıları daha karmaşık hale gelmiş, finansal mühendislik uygulamaları koruma (hedging) amaçlı yapılandırılmış ürünlerin risk yönetiminde kullanılmasına olanak sağlamıştır. Her ne kadar türev ürünler riskten korunmak amacına hizmet etse de bir yanıyla da spekülatif faktörlerle de hareket imkanı sağladığı için türev ürünlerden kaynaklanan riskler artmaya başlamıştır[9]. Türev ürünlerin giderek daha fazla kullanılmaya başlanması ve yazılım sektöründeki ilerlemelere karşın kontrol mekanizmalarını artırmak amacıyla risk yönetim tekniklerinin kullanımı önem kazanmıştır.

1.1.2. Finansal Piyasalarda Risk Türleri

Finansal piyasalarda risk en genel anlamda, olaylar ya da devam etmekte olan süreçler nedeniyle gelecekte zarara uğrama veya gelecekte elde edilecek gelirde değişkenlik yaşama ihtimali olarak tanımlanabilir. Finansal kuruluşların karşı karşıya olduğu riskler piyasa riski, kredi riski, likidite riski, operasyonel risk ve yasal riskler olarak sınıflandırılabilir.

Piyasa riski, bir finansal işletmenin mali yapısının, piyasa fiyatlarındaki dalgalanmalardan veya piyasalardaki zıt yönlü fiyat hareketlerinden dolayı maruz kalabileceği içinde faiz oranı riski, kur riski gibi riskleri barındıran hibrit bir risktir.

Kredi riski, bir sözleşmenin gereklerini karşı tarafın sözleşmede yer alan koşullara uygun olarak yerine getirmemesi ve geri ödeme kaynaklarının zararı karşılamaya yetmemesi durumu kredi riski olarak adlandırılır[10].

---

[9] K. Evren Bolgün ve M.Barış Akçay, **Risk Yönetimi Gelişmekte Olan Türk Finans Piyasasında Entegre Risk Ölçüm ve Yönetim Uygulamaları,** 2.Baskı, İstanbul:Scala Yayıncılık, Haziran 2005,. s.37-43.

[10] Niyazi Berk, **"Bankacılıkta Pazara Yönelik Kredi Yönetimi",** 3.basım, İstanbul: Beta Basım Yayın Dağıtım, Mart 2001, s.183.

Likidite Riski, bir işletmenin nakit akışındaki dengesizlikler sonucunda nakit çıkışlarını tam olarak ve zamanında karşılayacak düzeyde ve nitelikte nakit mevcuduna veya nakit girişine sahip olmaması riskidir.

Yasal Risk, bir işletmenin gerek iç yapısında, gerekse dışarıdaki kişiler ile yapmış olduğu işlemlerin yasal yollardan takip edilebilecek niteliklere haiz olup olmamasından dolayı maruz kalabileceği risktir.

Operasyonel Risk, tüm bu riskler içinde ölçümü ve yönetimi için geliştirilen teknikler açısından en gelişmemiş risk türüdür. Operasyonel risk kavramı diğer risklere göre literatüre en son girmiş, diğer bir deyişle adı en son konulmuş risklerden biridir. Genellikle kredi ve piyasa riski üzerinde çalışan ve bu risklerin etkilerini azaltma eğiliminde olan bankalar, yaşanan çok sayıda finansal kriz sonrasında operasyonel riskin varlığını kabul etmiş ve bu riski risk yönetimi kapsamına almışlardır[11]. Operasyonel risk insan, sistem, süreç *ve* dışsal faktörlerden kaynaklanabilmektedir. Operasyonel risk ve kaynakları ileride ayrıntılı olarak belirtilmektedir.

1.2. Operasyonel Risk Kavramı ve Tanımı

Bundan en az 20-30 yıl önce iş dünyasının temel söylemi: *"Önce iş yapalım, sonra gerekli önemleri alırız"* şeklindeydi. Fakat günümüz iş ve finans dünyasında ise yukarıdaki söylem şu hali almıştır: *"Önce riski ölç, sonra işe giriş".* 80'lerle beraber artan globalleşme ve teknolojik gelişmelerin iş ve finans dünyasını dönüştürmesi ve artan rekabet koşulları çerçevesinde hissedarların etkinliği ve önemi giderek daha fazla önem kazanmaya başlamıştır. Operasyonel riskin giderek önem kazanması da kurumun maruz kalacağı risklerin en iyi şekilde yönetilmesini, gelir getiren operasyonların faize, piyasa koşullarına, karşı taraf riski gibi farklı risk türleri karşısında daha korunaklı olmasını sağlamayı ve risk kaynaklı bir kayba dönüşmemesini sağlayarak hisse değerini, kurumun kar üretme kapasitesini artırmayı amaçlamıştır[12].

[11] Dilek Leblebici Teker, **Bankalarda Operasyonel Risk Yönetimi Örnek Banka Uygulamalı,** 1.Baskı, İstanbul:Literatür Yayınları, 2006, s.8.
[12] Jack L. King, **Operational Risk: Measurement and Modelling,** John Willey and Sons, Sussex: 2001, s.1-9.

Risk yönetimi, zaten finansal kurumların çok öncelerden beri üzerinde durdukları bir unsurdur. Çünkü paranın temel araç olduğu bir ortamda riskin olmayacağı düşünülemez. Fakat günümüzde risk yönetimi, özellikle finansal kurumlarda daha fazla önem kazanmıştır. İyi işleyen bir risk yönetimi sistemi, kuruma istikrar ve devamlılık sağladığı gibi gelir üretimini artırıp olası giderleri önleyerek de üst yönetimin kendilerinden beklenenleri karşılamalarına yardımcı olmaktadır. Bu çerçevede 1988 yılında Basel Komitesi ilk Basel Uzlaşısı'nı ortaya koyarak finansal kurumların kredi ve piyasa riskine göre yeterli olacak sermaye düzeyini sağlamalarını öngörmüştür. Basel-II Uzlaşısı daha önce sektörde net bir şekilde tanımlanmamış olan operasyonel riski tanımlayarak kurumların yeterli sermaye düzeyini tesis etmelerini öngörmektedir.

Her ne kadar tüm sektör ve akademik dünya tarafından üzerinde uzlaşılmış bir operasyonel risk tanımı olmasa da düzenleyiciler ve sektör temsilcileri arasında gerçekleşen uzun tartışmalar neticesinde Basel Komitesi'nin tanımı oldukça geniş bir kabul görmüştür[13]. Komite operasyonel riski *"yetersiz veya başarısız iş süreçlerinden, personelden, iç sistemlerden ve dışsal faktörlerden kaynaklanan risk"* olarak tanımlamış ve yasal riski tanım kapsamına dahil ederken, repütasyon riskini ve iş/strateji riskini tanım içine almamıştır[14]. Bu tanım esas olarak operasyonel kayba ilişkin olarak sebepleri, olayları ve ortaya çıkan sonucu tanımlamayı esas almaktadır. Örneğin, kurum içinde iç kontrol sistemin zafiyetinden kaynaklanan (sebep) bir yolsuzluk/dolandırıcılık (olay) maddi değeri olan bir kayba sebebiyet vermekte (kayıp) ise bu şekilde bir tanımlama sürecini içermektedir.

Ülkemizde de BDDK tarafından 2001 yılında yayımlanan "Bankaların İç Denetim ve Risk Yönetimi Sistemleri 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 kayıplar ya da zarara uğrama ihtimali"* olarak tanımlanmıştır.

[13] Douglas Hoffman, **Managing Operational Risk**, John Willey and Sons, NewYork:2002, s.29-31.
[14] Douglas G. Hoffman, **Managing Operational Risk: 20 Firmwide Best Practice Strategies,** New York:Wiley, 2002, s.30.

1.2.1. Operasyonel Risk Yönetiminin Artan Önemi

Finansal piyasalarda yaşanan skandalların geçmiş dönemlere kıyasla son yıllarda artmasıyla operasyonel risk de giderek önem kazanan bir ilgi alanı olmaya başlamıştır. Finansal piyasalarda faaliyet gösteren tüm kurumların daha fazla bir şekilde teknolojiye olan bağımlılığının artması, finansal kurumlar arasında giderek artan rekabet ortamı ve finansal piyasalarda ortaya çıkan globalleşme sonucunda finansal kurumlar giderek operasyonel riske daha fazla maruz kalmaya başlamışlardır. Bu konuda Amerika'da gerçekleştirilen bazı anket çalışmaları[15] kurumların maruz kaldığı operasyonel riskin sıklığı ve önemi konusunda bazı bilgiler sunmaktadır. Şubat 2006 da 350 adet şirket ile ilgili olarak gerçekleştirilen risk çalışmasında katılımcıların %68'i bir çeşit ödeme sırasında dolandırıcılıkla karşılaştığını ve ankete cevap veren kurumların %54'ü ise ödemelerin kontrolüne ilişkin olarak ciddi yeniden yapılanmalar gerçekleştirdiklerini belirtmişlerdir. Yine 1997 yılında British Bankers Association'ın Coopers & Lybrand iş birliği ile bankaların operasyonel riske ilişkin değerlendirmelerini ölçmek amaçlı olarak gerçekleştirilmiş olan çalışmaya[16] sektörde faaliyet gösteren 45 adet firma katılmıştır. Çalışmaya dahil olan kurumlar sektörün hemen hemen her alanında faaliyet gösteren kurumlar olarak seçilmiş olup perakende bankacılıktan, yatırım bankacılığına, takas ve saklama hizmetlerinden fon yönetimine, hazine işlemlerinden sermaye piyasası faaliyetlerine kadar geniş bir spektrumu içermektedir. Çalışmanın bulguları kısaca şunlardır: kurumların %67'den fazlası operasyonel riskin en az piyasa riski ve kredi riski kadar önemli olduğunu, %24'ü son 3 yıl içinde en az 1 milyon pound'dan az olmayan kayba uğradığını, % 47'si sermaye piyasası ve hazine işlemlerinin iş kolu olarak en fazla risk yaratabilecek bölümler olduğunu, % 33'ü maruz kalınan operasyonel riskin etkisini ve maliyetini ölçmediğini, % 62'si ise de gelecek iki yıl içinde operasyonel riske bakış açılarını değiştirmeyi düşündüklerini belirtmişlerdir.

Operasyonel riskin finansal kurum açısından giderek önem kazanmasında globalleşmeden farklılaşan müşteri isteklerine, değişen piyasa yapısından artan teknolojik imkanlara kadar birçok etken rol almıştır[17].

---

[15] Imad A. Moosa, **Operational Risk Management**, Eeastbourne:Palgrave Macmillan, 2007, s.77-78.
[16] Amanat Hussain, **Managing Operational Risk in Financial Markets,** Oxford; Boston: Butterworth-Heinemann, 2000, s.70-71.
[17] Chris Frost, David Allen, James Porter and Philip Bloodworth, **Operational Risk and Resilience,** Boston:Butterworth-Heinemann, 2001, s.230-233.

Operasyonel riskin giderek daha fazla önem kazandığını gösteren önemli göstergelerden biri ise Basel Komitesinin yönlendirici kararlar alırken operasyonel riske daha fazla önem vermeye başlamasıdır. Komitenin geçmişi ve ortaya koyduğu çalışmalar, başlangıçta kredi riskine daha fazla önem verildiğini, daha sonra piyasa riskine de önem vermeye başladığı ve özellikle Basel II düzenlemelerinde üzerinde durulan diğer bir noktanın ise operasyonel risk olduğunu görülmektedir.

1.2.2. Operasyonel Riskin Karakteristiği

Operasyonel risk tanımı altında yer alabilecek unsurların çeşitliliği ve sayısal olarak çokluğu, bu riskin anlaşılmasını daha net bir şekilde tanımlanmış piyasa ve kredi riskine göre zorlaştırmaktadır. Yasal uyumdan doğal felaketlere kadar çok geniş bir spektrumu kapsamakta olan operasyonel riskin bu çeşitliliği gerek açıkça tanımlamasını gerekse de sınırlarının net bir şekilde çizilmesini zorlaştırmaktadır. Çünkü operasyonel risk, bir kurumun ön ofisten başlayıp arka ofis ve diğer tüm destek ünitelerini de kapsayan bir risk türüdür. Dolayısıyla operasyonel riski tanımlamak, diğer risk türlerini tanımlamaktan daha zordur. Buchet ve Untregger operasyonel riski *"hayli değişik ve birbiriyle ilişkili olan ve değişik kaynaklardan gelen riskler seti"* olarak tanımlamışlardır[18].

Kredi ve piyasa riskine ilişkin olarak risk toleransını belirlemek için çok çeşitli metotlar kullanılabilir (örneğin risk yoğunlaşması ya da VaR-Value at Risk- bazlı metotlar). Ama günümüzde benzer şekilde operasyonel riske yönelik olarak belirlenmiş ve kabul edilebilir limitler, hesaplamaya dönük yeterince test edilmiş ve kendilerini yeterince kanıtlamış modeller maalesef yoktur.

Operasyonel riskin diğer bir özelliği ise "tek-taraflı" olduğu yönündeki eleştirilerdir. Operasyonel risk, piyasa yada kredi riski gibi herhangi bir risk-getiri ikilemi sunmamakta, sadece karmaşık operasyonel faaliyetlerde ortaya çıkan istenmeyen bir sonuç olarak görülmektedir. Çünkü piyasa yada kredi riskinde olduğu gibi daha fazla operasyonel riske maruz kalınarak daha fazla getiri elde edilmesi söz konusu değildir[19]. Her ne kadar bu

[18] R Buchelt ve S. Unteregger, "Cultural Risk and Risk Culture: Operational Risk After Basel II"**,** 2004, Financial Stability Report 6'dan Moosa, s.77-79.
[19] Michel Crouhy, Dan Galai ve Robert Mark, **Risk Management [electronic resource],** New York: McGraw Hill, 2000 ve Diğerleri, s.163-165.

tespitler operasyonel riskin farklı yönlerini gösterse de aslında operasyonel riski yönetmek isteyen ve bunun için ciddi yatırımlar yapan kurumların hedeflerinin aynı zamanda daha az kayba uğrayarak getiri hacimlerini artırmak oldukları söylenebilir.

Amaç operasyonel riski sıfırlamak ise, bunun tek yöntemi faaliyetleri bir anda sonlandırmaktır ki faaliyet yoksa getiri de olmayacak ve getirileri etkileyecek operasyon kaynaklı bir risk de doğmayacaktır. Ama finansal kurumların operasyonel riske maruz kalarak bunu bir getiri üretmek için yapmaları aslında tam anlamıyla ”çift yönlü” bir ikilemdir.

1.3. Operasyonel Riskin Kaynakları

Operasyonel riskin özelliği tüm sektörlerde olduğu gibi finans sektöründe de her zaman mevcut olmasıdır. Örneğin henüz yeni kurulmuş bir banka, bir tek kredi vermeden bile operasyonel riske maruz kalabilir. Operasyonel risk genel olarak içsel etmenlerle ilişkili olsa da, dışsal etmenler de dikkate alınmalı ve hatta gereken ve mümkün olan ölçüde sigortalanmalıdır.

Bir finansal kurumdan hizmet almayı bekleyen müşterilere karşı sunulması gereken hizmetlerin zamanında ve hatasız olarak sunulamaması, zimmet, dolandırıcılık nedeniyle yaşanan mali kayıplar, operasyonel risklerin kurumsal yönetim süreçlerinde veya bu süreçlerin iç kontrol aşamalarında gerçekleşen kontrol zafiyetlerden kaynaklandığını göstermektedir. Diğer taraftan bilgi sistem teknolojilerinin sektörde giderek çok daha fazla yoğun şekilde kullanmasından kaynaklanan ya da bankanın tamamen elinde olmayan sebeplerden kaynaklanan yangın, sel, deprem gibi doğal felaketler de benzer şekilde mali kayıplara yol açabilmektedir. Tablo 1’de önemli kayıplara neden olmuş operasyonel risklere örnekler verilmiştir.

Tablo 1: Operasyonel Risk Kaynaklı Kayıplara İlişkin Örnekler

KURUM	OLAY	YIL	ZARAR ($ milyon)
Daiwa Bank, New York	Zayıf yönetim kontrolleri nedeniyle gerçekleşen yetkisiz tahvil işlemleri	1984-95	1.100
Sumitomo Corp, London	Yetkisiz işlemler, yolsuzluk ve sahtecilik	1986-96	1.700
UK Yaşam Sigortası Sektörü	Prim sahtekarlığı	1988-94	18.000
Standard Chartered, Hindistan	Bombay Menkul Kıymet Borsası'nda usulsüzlükler	1992	400
Credit Lyonnais	Zayıf kredi kontrolleri	1980ler-1990lar	29.000
ABD Bankaları, Şirketleri ve Parekendecileri	Çek Yolsuzluğu	1993	12.000
Londra Menkul Kıymetler Borsası ve Üye Şirketler	TAURUS Sisteminin çökmesi	1993	700
Kidder Peabody	Tahvil Ticareti, yetersiz iç kontroller	1994	200
Procter& Gamble	Yönetim hataları	1994	157
Morgan Grenfell	Hatalı muhasebe kayıtları	1990lar	640
Orange County	Tahvil ticareti, eksik yönetim kontrolleri	1994	1.700
Barings, Singapur	Türev işlemlerinde yetersiz kontrol ve görevlerin ayrılma ilkesindeki yetersizlikler	1995	1.600
Deutshe Bank (Morgan Grenfell), Londra	Yetkisiz yatırım kararları	1996	600
eBay	Teknoloji problemleri	1999	Piyasa değerinde 5.000 düşüş

Kaynak: Evren Bolgün ve Barış Akçay, **"Risk Yönetimi Finansal Piyasalarda Risk Ölçüm ve Yönetimine Türkiye Perspektifinden Stratejik Bakış"**, İstanbul:Scala, 2003.,s.608-609.

Finansal kurumların her birini etkileyen makro düzeyde operasyonel riskler olsa da, operasyonel risklere yol açan faktörler her kurumun kendi iç yapısına ve faaliyetlerine göre farklılık arz etmektedir. Operasyonel riskin kaynakları genel olarak bir sınıflandırmaya tabi tutulursa bu risk; insan, sistem, süreç ve dışsal faktörler olarak dört başlık altında değerlendirilebilir.

1.3.1. İnsan

Merkezinde insan olan riskler doğası gereği en belirsiz olan dinamik bir risk kategorisidir. Operasyonel riskler çoğu zaman sistemsel ve işlem bazlı hatalar olarak görünse de birçok hatanın ve riskin doğmasında doğrudan ya da dolaylı olarak insan faktörünün etkisi vardır. Her kurum, insan kaynağının kendileri için en değerli varlık olduğunu belirtse de insan kaynaklı gerçekleşen veya gerçekleşme olasılığı olan riskleri ölçmek ve belirli modeller oluşturmak hiç de kolay bir iş değildir.

Herhangi bir kurumda insan unsurundan kaynaklanan çok çeşitli risk doğurucu etmen sayılabilir. İnsan kaynaklı riskler ana hatlarıyla; personelin nicel olarak sayısına ilişkin sıkıntılar, nitel olarak yetersizliğine ilişkin sorunlar, iş ahlakına aykırı olarak dolandırıcılık içinde bulunması ve risk kültürünün gelişimine önem vermeyen bir kurumsal bakış olarak kategorize edilebilir[20].

Operasyonel riske, sadece alt seviyede kurumun rutin işlemlerinden sorumlu personel tarafından gerçekleştirilmesi muhtemel riskler olarak bakılması, insan merkezli olası kayıpların yüzeysel bir şekilde incelenmesine sebep olur. Kurumların üst seviyelerinde çalışan yönetici konumundaki personelin de operasyonel risk kaynaklı mali kayıplara sebep olma potansiyeli vardır. Örneğin Enron kaynaklı mali skandaldaki payları çerçevesinde JP Morgan Chase 135 milyon $ ve Citigroup da 120 milyon $ ABD Menkul Kıymet Denetim Otoritesi'ne (SEC:Securities and Exchange Commission) ceza ödemişlerdir.[21] Bu çapta bir cezayı ödemek zorunda olan kurumun ciddi büyüklükte bir operasyonel riske maruz kaldığı açıktır.

Kurumun yönetici konumundaki personelinin bazen kasten yasalara ve iş ahlakına aykırı olarak kendilerini bir çıkar çatışmasının içinde kişisel menfaat temin edebilecekleri bir ortamda bulmalarından dolayı bazen de iyi niyetle verdikleri yanlış kararlar neticesinde kurum aleyhine riskli durumlar ortaya çıkabilmektedir.

1.3.2. Sistem

Teknoloji ve bilgi sistemlerinin gelişmesine ve iş dünyasında daha önce benzerine az rastlanır şekilde kullanılmaya başlanmasıyla beraber bilgi sistemleri kaynaklı operasyonel risk olayları da giderek artmıştır. Günümüzde bir çok kurum tüm faaliyet alanları ve iş kolları bazında entegre bilgi sistemleri kullanmakta, birçok hizmetini dışsal servis sağlayıcı kurumlardan tedarik etmekte ve bazen de farklı kurumlarla ortak pazarlama gerçekleştirmek amacıyla veri tabanı paylaşımında bulunmaktadır. Teknoloji ile iç içe olan bu kurumlar piyasada gerçekleşen gelişmelere bağlı olarak sistemlerini

[20] James Lam, **Enterprise Risk Management: From Incentives to Controls,** John Wiley and Sons, 2003, s.212.
[21] Ioannis Akkizidis, and Vivianne Bouchereau, **Guide to Optimal Operational Risk and Basel II**, New York:Auercbach Pub., 2006ve Bouchereau, s.15.

zamanında güncelleyemezse ve sektör standartlarından geride kalırsa ciddi bir iş ve bilgi sistemleri riskine maruzdurlar.

Bilgi sistemleri riski özellikle bir güven kurumu olarak faaliyet gösteren bankalar için çok daha önemli bir konudur. Banka, sistemindeki bir hata ya da genel olarak sistem kapasitesinin mevcut faaliyet yükünü karşılayamaması sonucu, operasyonel riske maruz kalabilir. Sistemden kaynaklanan riskler üç ana kategoride toplanabilir.

a) Genel Riskler,
    i. Yetkisiz erişim,
    ii. Değişim yönetimi,
    iii. Kapasite yönetimi ve arttırma,
    iv. Acil durum yönetimi
b) Uygulama Odaklı Riskler
c) Kullanıcı Odaklı Riskler

Genel riskler incelendiğinde, yetkisiz erişimler çok ciddi bir güvenlik sorunu olarak ortaya çıkmaktadır. Bankaların sürekli olarak itibara dayalı iş yapmaları nedeniyle, maddi ve itibar kaybına neden olabilecek bu tarz risklerden korunmak için yatırımlarını eksiksiz yapmaları gerekmektedir. Fakat gelişen teknolojik olanaklar, bu konuda suç işleme amacında olan kötü niyetli kişilerin ve suç gruplarının önüne önemli araçlar sunmaktadır. Banka sistemlerinin korumalı olmadığı durumlarda, diğer kullanıcılar rahatlıkla sisteme müdahale edebilir veya sistem içinde yer alan verilere erişebilirler. Sistemdeki bu aksaklık sonucu, gerek banka içi gerek banka dışı kullanıcılar sisteme girerek hesaplara yetkisiz erişimler gerçekleştirebilirler.

Değişim yönetiminin amacı, banka sisteminin değiştirilmesi ya da piyasadaki gelişmelere uyum sağlamak için yüklenen yeni bir yazılımın banka verilerine zarar vermesini önlemektir. Bankada yeni kullanılmaya başlanan bir yazılım ya da sistemde yapılan bir güncelleme ile banka verileri zarar görebilir[22]. Sistem ile ilgili ortaya çıkabilecek bir başka sorun ise bankanın yerel ve merkezi yazılımlarının birbirine bağımlı olması sonucu merkezi sisteme yerleştirilebilecek yeni bir yazılımın tüm yerel birimleri etkilemesi

[22] Provident Finacial Group yeni bir finans modelini kullanmaya başladıktan sonraki süreçte oluşan yanlış hesaplamalar neticesinde, gelirlerin olduğundan 70.3 milyon $ daha fazla gösterildiği, 2003 Şubat ayında bir personelin hatayı fark etmesi üzerine tespit edilebilmiştir. Akizidis ve Bouchereau, s.13-14.

ve işlerin aksamasıdır. Etkin bir değişim yönetimi, uygulanacak olan bu yeni yazılımların sistemde yaratacağı etkileri iyi saptayabilmelidir.

Kapasite yönetimi, sistemin bileşenlerini inceleyerek oluşacak sorunları önlemeyi amaçlar. Ortaya çıkacak bir hata, network, iç bellek, dış bellek ya da veritabanından kaynaklanabilir. Eğer bunlardan birinin kapasitesi yetersiz ise, işlem süreci yavaşlar ya da çökebilir. Örneğin, bankanın Reuters sisteminin çöktüğü varsayılırsa hem banka hem de aracılık ettiği müşterisi piyasa verilerine ulaşamaz. Bu süre içinde piyasada büyük dalgalanmaların olması durumunda, söz konusu banka kayıplara uğrayabilirken müşterilerinin de kaybını telafi etmek durumunda kalabilir[23].

Acil durum yönetimi (Emergency Management) kapsamında, bankaların tüm operasyonel birimlerinin, kendi alanları için acil durum ve iş süreklilik planları hazırlamaları gerekir. Birçok düzenleyici otorite de bankaların ortaya çıkması olası kayıplarını belirlemeleri ve bunlara ilişkin acil durum ve iş sürekliliği planlarını hazırlamalarını öngörmüştür. Felaketsel olayların sonunda bankalar doğrudan ve dolaylı birçok kayba maruz kalabilirler. Örneğin yaşanacak bir yangın, deprem, soygun ya da terör saldırısı sonrasında tüm banka çalışanlarının uymaları gereken önceden planlanmış bir acil durum ve iş süreklilik planı olması gerekmektedir.

Uygulama-odaklı riskler (Application-oriented risks), sistemde yaşanan aksaklıklar dolayısıyla veri girişinin yanlış yapılması, verinin geçerli olduğu süre içinde saklanmaması, hazırlanan raporlarda geçerli bilginin bulunmaması, hesaplama hataları, sistem hataları dolayısıyla bilgi akışının zamanında yapılmaması gibi nedenlerden dolayı ortaya çıkabilmektedir. Örneğin 20 Kasım 1985 tarihinde Bank of New York Amerikan hazine bonolarının netleştirme işlemi sırasında normale göre 32,000 adet fazla işlem gerçekleştirerek bir rekor kırmıştır. Bu rekor işlem sayısı, uygulama yazılımının hata yapmasına sebep olarak bonoların asıl alıcıların hesabına geçmesini engellemiş, bir gün sonrası ise takas günü olduğu için Banka alıcılara teslim edemediği bonoları kendisi finanse etmek zorunda kalmış bu yüzden Amerika Merkez Bankası'ndan (FED:Federal Reserve) 23 milyar $ borçlanmak durumunda kalmış; sistem ancak bir gün sonra düzeltilebilmiştir. Örnekte de görüldüğü gibi netleştirme ve takas operasyonlarında oluşan

[23] Teker, s.31-32.

yüksek hacimli işlemlerde gerçekleşecek bilgi sistem kaynaklı en ufak bir risk bile kurumlara çok büyük zararlar doğurabilmektedir[24].

Kullanıcı odaklı riskler, önemli ölçüde "insan" riski ile ilişkilidir. Genellikle çalışanların, bilgisayar sistemi ile ilgili bilgi eksikliğinden kaynaklanmaktadır. Kullanıcı odaklı riskleri azaltabilmek için, özellikle yapılan işlemin çalışan tarafından yürütülen aşamasını incelemek ve kontrol sistemleri geliştirmek gerekmektedir[25].

Sistem kaynaklı riskler, bilgisayar donanımlarında, yazılımlarında, bilgi depolama ve iletişim sistemlerinde yaşanan yetersizlikler veya aksaklıklardan kaynaklanan risklerdir. Kasıt unsuru taşımayan aksaklıklardan ötürü ortaya çıkan söz konusu riskler ve zarar olayları bu gruba dahil edilmekte, kurum içi kasıtlı eylemler sonucu oluşan riskler personel riski, bilgisayar sistemlerine yapılan kurum dışı saldırılar ise dış riskler kapsamında değerlendirilmektedir[26].

1.3.3. Süreç

Süreç kaynaklı operasyonel risk aslında temel olarak etkin olmayan ve verimsiz olan süreçlerden kaynaklanır. Etkin olmayan süreç; tasarlanan amaçları gerçekleştirmeyen süreçtir. Verimsiz olan süreç ise, tasarlanmış olduğu amacı gerçekleştirse de göreceli olarak ve sağladığı fayda göz önünde bulundurulduğunda oldukça maliyetli olarak gerçekleştiren süreçtir[27]. Doğal olarak iki terim arasında bir karışıklık, çelişki vardır. Örneğin, iş süreçlerini daha az maliyetli hala getirmek için girişilen yeniden yapılandırma modellerinin (reengineering modelling) temel amacı maliyeti aşağı çekmek olduğu için temel bazı kontrol noktalarını devre dışı bırakarak belki de kazanılan maliyet avantajından çok daha yüksek miktarda riske maruz kalınabilmektedir. Dolayısıyla, herhangi bir süreci tasarlarken ve yeniden gözden geçirirken kontrollerin de etkin şekilde çalışıyor olmaları ve iki kavram arasında işlevsel dengenin sağlanması gereklidir.

---

[24] Akizidis ve Bouchereau, s.13-14.
[25] Bolgün ve Akçay, s.608-609.
[26] Dimitris N. Chorafas, **Operational Risk Control With Basel II: Basic Principles&Capital Requirements,** Boston:Elsevier Butterworth-Heinemann, 2004, s.90-93.
[27] Lam, s.211.

Finansal kurumlar müşterilerine hizmet sunmak için çok sayıda süreç ve ürün kullanmak zorundadırlar. Dolayısıyla, müşteriye sunulan bir artı değer için sürecin herhangi bir aşamasında yaşanan riskler ve hatalar bankalar için çok çeşitli maliyetlere sebep olabilmektedir. Örneğin, kredi kampanyaları kapsamında gönderilen kısa mesajlar (SMS mesajları), elektronik postalar ya da gönderiler gerçekten o tür hizmetlere ihtiyacı olmayan müşterilere hatta bankanın müşterisi olmayan kişilere bile ulaşabilmektedir.

Operasyonel riske sebep olabilecek süreçler yedi alt grupta sınıflandırabilir: ödeme ve teslimat riski, belgeleme ve sözleşme riski, banka içi ve banka dışı raporlama riski, proje riski ve değişim yönetimi, satış ve hizmet riski, banka sistem ve varlıklarının kontrolü, görev tanımı ve yetkilerin belirlenmesi[28]. Daha genel bir çerçevede süreç ile ilgili riskler incelenecek olursa, kurum faaliyetlerinin işleyişi ile ilgili süreçlere ve süreçleri tamamlayıcı fonksiyona sahip iç kontrollere ilişkin prosedürlerin olmaması, mevcut prosedürlerin yanlış tasarlanması ya da yanlış şekilde uygulanması süreç kaynaklı risklerin sebebi olarak sayılabilir. Kurum içi birimler arasında bilgi akışındaki yetersizlikler, yetkilere ilişkin sınırların açık olarak belirlenmemesi, yeterli ve etkin kontrol mekanizmalarının olmaması yanında, kurumun maruz olduğu risklerin saptanmaması ve kurum çalışanlarının riskler konusunda yeterince bilgilendirilmemesi gibi hususlar bu gruba dahil olan risklere yol açan faktörler arasında yer almaktadır.

1.3.4. Dış Kaynaklı Riskler

Kurumların belki de kontrol noktası olarak en az etkin olabileceği risk kaynağı, kurum harici gelişen olaylardan kaynaklan kayıplardır. Bu gruba giren riskler;

a) dışarıdan alınan hizmetlerden kaynaklanan riskler,
b) banka dışı riskler,
c) doğal afetler

olmak üzere üç başlık altında incelenebilir.

Dışarıdan alınan hizmetlerden kaynaklanan riskler son yıllarda oldukça önemli bir boyut kazanmıştır. Dışarıdan hizmet alınmasının (outsourcing) genel amacı, maliyetlerin

[28] Teker, s.32-33.

düşürülmesi ve maruz kalınacak risklerin azaltılması düşüncesidir. Ancak bazen dışarıdan alınan bir hizmet, beklenmeyen risklere de yol açabilmektedir. Örneğin temin edilen hizmet ile hedeflenen kalite standardının birbirini tutmaması veya bankacılık sırrı kapsamındaki bilginin yetkisiz kişilerin eline geçmesi gibi[29].

Banka dışı riskler; terörist saldırılar, kara para aklama ve banka dışı faktörlerden kaynaklanan riskleri içermektedir[30]. Küreselleşme ve teknolojide yaşanan gelişmeler sonucu finansal kuruluşların uluslararası faaliyetlerinin artmasına bağlı olarak, kurum faaliyetlerinin, ürün ve hizmetlerinin birden fazla hukuki düzenlemeye tabi olmasından kaynaklanan riskler yasal riskler kapsamındadır[31]. Ayrıca, kurum ile müşteriler veya hizmet alınan kurumlar arasında çıkan ihtilaflar nedeniyle taraf olunan hukuki davalar da yasal risk kapsamındadır[32].

Dışsal risklerin bir diğer grubunu da doğal afetler oluşturmaktadır. Yaşanacak deprem, sel, yangın, kapsamlı elektrik kesintisi gibi felaketler, bankaların sistemlerine oldukça büyük zararlar verebilirken yine aynı felaketler bankaların arşivlerinde ciddi kayıplara neden olabilirler. Bu tür yıkıcı risklerden korunmak için bankalar genellikle bu kayıplarını sigortalamaktadırlar.

1.4. Yasal (Düzenleyici) Çevre ve Tavsiye Kararları

Risk yönetimi ve sermaye yeterliliği konularında ulusal/uluslararası alanda alınan kararların bir kısmı tavsiye niteliğinde iken, bir kısmı da düzenleyici otoritenin yayımladığı ve uyulmak zorunda olunan mevzuat hükmündedir.

Uluslararası Menkul Kıymetler Komisyonu (IOSCO: International Organization of Securities Commissions) ve Otuzlar Grubu (G-30: Group Thirty) olarak adlandırılan ve türev piyasalarda yaşanan sorunların ardından özel sektörden, kamu kurumlarından ve akademik dünyadan üst düzey katılımcılardan oluşmuş olan komisyonun yayımladığı

[29] Teker, s.12.
[30] Terörist saldırıların oluşturduğu en büyük mali kaybın New York kentinde faaliyet gösteren tüm kurumlara maliyeti yaklaşık 16.9 milyar $'ı bulan 11 Eylül saldırılarıdır. Bu maliyeti oluşturan alt kalemler ise faaliyetlerin durmasından, piyasanın kapanmasından ve taşınma maliyetinden kaynaklanan toplam tutardır. Bunun dışında hayatlarını kaybeden personelin entelektüel birikimi ve deneyimi ise çok daha farklı bir maliyet kalemini teşkil etmektedir. Akizidis ve Bouchereau, s.15-16.
[31] Hussain, s.89.
[32] Chorafas, s.49.

kararlar da tavsiye hükmündedir. Diğer yandan yaşanan Enron benzeri finansal skandallardan sonra kurumsal yönetim ilkelerinin ayrılmaz bir parçası olarak ABD'de yayımlanan Sarbanes Oxley Kanunu (SOx), şirketlerin uymak zorunda olduğu yasal bir düzenlemedir.

Basel Komitesi tarafından oluşturulan Basel-I ve Basel-II (International Convergence of Capital Measurement and Capital Standards) Uzlaşıları tavsiye niteliğinde yayımlanmış kararlar olmasına rağmen birçok ülkede olduğu gibi ülkemizde de bu kararlar, bankacılık alanında ulusal düzenleyici ve denetleyici otorite olan BDDK tarafından bankalarca uyulmak zorunda olunan mevzuat hükmüne getirilmiştir. Aynı şekilde Avrupa Birliği de 2006/48/EC ve 2006/49/EC sayılı Direktifler ile AB müktesebatına dahil edilmiş ve söz konusu Direktifler belirli bir geçiş süreci dahilinde AB üyesi ülkelerde uygulamaya konulmuş olup hali hazırda dünya çapında bir çok ülkede ise Basel-II 'ye uyum çalışmaları devam etmektedir[33].

1.4.1. IOSCO Düzenlemeleri

1983 yılında kurulmuş olan IOSCO, ABD'deki Sermaye Piyasaları Komisyonu (SEC: The Securities&Exchange Commission), İngiltere'deki Finansal Kurumlar Otoritesi (FSA: Financial Services Authority), Türkiye'deki Sermaye Piyasası Kurulu (SPK) ve bunlara benzer toplam 182 üyeli[34] ulusal menkul kıymet düzenleme kurumlarının dünya çapındaki birliğidir.

IOSCO sermaye piyasalarındaki düzenleyici/denetleyici otoritelerin, ilgili alanlarda koordinasyonu ve işbirliğini sağlamak, sermaye piyasaların yasal ve kurumsal yapısına ilişkin olarak ortak uluslararası standartlar oluşturmak ve üyeler arasında bilgi alış verişini olanaklı kılmak amacıyla oluşturdukları bir kuruluştur. IOSCO, mali piyasalarla ilgili diğer uluslararası kuruluşlarla da işbirliği halinde faaliyet göstermekte ve alanındaki en etkin uluslararası kuruluş olma niteliğini taşımaktadır[35].

---

[33] BDDK, **Bankacılık Sektörü Basel II İlerleme Raporu**, Mayıs 2009, s.1.
[34] http://www.iosco.org/about/ (08 Nisan 2008).
[35] Cemal İbiş ve Ayça Akarçay, "IOSCO Deklarasyonu ve Menkul Kıymet Borsalarında IAS'ın Uygulanması Süreci", Marmara Üniversitesi, İİBF, s.2.

IOSCO Teknik Komitesi tarafından 1998 yılında yayınlanmış olan *"Aracı Kurumlar ve Denetleyici Otoriteler için Risk Yönetimi ve Kontrolü"* adlı Rapor[36], aracı kurumlar ve bu finansal kurumları denetlemeye yetkili olan otoriteler için bir rehber niteliğinde olup, aracı kurumların sahip olması gereken risk yönetimi sistemleri ve iç kontrole dönük politika ve prosedürlerine ilişkin bazı temel kavramları içermektedir.

Rapor aracı kurumların maruz kaldığı riskleri piyasa riski, kredi riski, likidite riski, operasyonel risk, sistemik risk olarak türlere ayırmıştır. Her birini ayrı ayrı tanımlamış ve son zamanlarda bahse konu risklerin gerçekleşmesi sonuncunda sektörde yaşanmış olan önemli kayıplara ilişkin örnekler verilmiştir. Rapor operasyonel riski ise, *"işlem süreçlerinin ve yönetim sisteminin uygun işlememesinden kaynaklanan finansal zarar"* olarak tanımlamıştır. Operasyonel risk tanımı kapsamında, limit aşımları, yetkisiz işlemler gerçekleştirilmesi, yolsuzluklar, arka ve ön ofis bölümlerinde yaşanan yolsuzluklar, muhasebeye dönük kontrollerinin olmaması, tecrübesiz personel çalıştırılması, sızmaya çok elverişli bilgi sistemlerinin bulunuyor olması gibi risk unsurları belirtilmiştir. Raporda, iyi bir operasyonel risk yönetimi için hesapların, kayıtların ve temel muhasebe kontrollerinin bulunması gerektiği, iyi işleyen ve gelir getiren bölümlerden bağımsız olarak yapılandırılmış olan bir iç denetim birimin bulunması gerektiği, net bir şekilde personel ve dealer bazında tanımlanmış limitlerin olması gerektiği belirtilmektedir[37].

1.4.2. G-30 Önerileri

G-30, özel sektörden, kamu kurumlarından ve akademik dünyadan üst düzey katılımcılardan oluşmuş bir komisyondur. G-30, 1990'larda türev piyasalarda yaşanan sorunların ardından, 1993 yılında türev piyasalarda işlem yapan dealerlar, yatırımcılar ve piyasanın düzenleyici ve denetleyici otoriteleri için toplam 24 maddeden oluşan risk yönetimi ile ilgili tavsiye niteliğinde kararlar yayımlamıştır[38]. Başlangıçta türev piyasalardaki risklere karşı yayımlanmış olan kararlar, sonradan tüm yatırım portföylerine uygulanmıştır[39].

---

[36] Evrim Can, "Operasyonel Risk ve Yönetimi", **SPK Yeterlik Etüdü**, Yayın No.154, Ankara: 2003, s.38.
[37] Can, s.38-41.
[38] Crouhy, ve Diğerleri, s.48.
[39] Philippe Jorion, **Value at Risk [electronic resource]: The New Benchmark For Managing Financial Risk,** New York: McGraw-Hill, c2001. s.484.

G-30 raporu, her ne kadar özellikle türev piyasalarda faaliyet gösteren piyasa oyuncularının riske bakış açısını geliştirmek için oluşturulmuş olsa da risk yönetimi ile ilgilenen tüm ilgili kişilere de hitap eden önemli bir referans kaynağı olarak kabul edilmektedir[40].

G-30 raporu kısaca; risk yönetiminin işlem yapan personelden ayrı bir yapı olması, üst yönetimin her zaman gözetleyici bir rolünün olması, görev ayrılığının net bir şekilde tesis edilmesi, çalışanların yeterli tecrübe ve donanıma sahip olması, teknolojik sistemlerin etkin bir şekilde çalışıyor olması gibi hususları içermektedir.

G-30'un yeni önerileri içerisinde menkul kıymet işlemlerinde otomasyonun artırılması ve tam otomasyon sağlanmasına yönelik olarak uluslararası menkul kıymet standartlarının kullanımı üzerinde önemle durulması dikkat çekmektedir[41].

1.4.3. Sarbanes-Oxley Kanunu

2001 yılı ve sonrasında ortaya çıkan Enron, Worldcom gibi büyük şirketlerin iflas etmeleri Amerikan sermaye piyasalarına olan güveni derinden sarsmış ve halka açık şirketlerin açıkladıkları mali tablolara yönelik kuşkuların artmasına sebep olmuş ve bağımsız denetim şirketlerinin iş yapış tarzları ve çalışma koşullarını belirleyen yasal çerçeve de sorgulanmaya başlanmıştır[42]. Güven bunalımın arttığı böyle bir ortamda 2002 yılında çıkarılan ve Sarbanes-Oxley Kanunu (SOx) olarak anılan "Bağımsız Denetim Şirketleri Reformu ve Yatırımcı Koruma Yasası"nın asıl amacı halka açık şirketlerce açıklanan finansal tabloların ve tüm yatırımcıları ilgilendirecek açıklamaların güvenilirliğini ve doğruluğunu artırarak yatırımcıları korumaktır. Yasanın ana omurgası bağımsız denetim şirketlerinin işleyişini düzenlemek ve halka açık şirketlerin gerçek mali durumlarını yansıtan finansal tablolarını açıklamalarını sağlamaktır. SOx, aynı zamanda operasyonel risk yönetiminin bir unsurunu oluşturan farklı alanlara ilişkin de düzenlemeler getirmiştir:[43]

---

[40] Karen A. Horcher, **Essentials of Financial Risk Management,** Hoboken, NJ, USA: John Wiley&Sons, Incorporated, 2005, http://site.ebrary.com/lib/boğazici (12 Eylül 2007), s.170-176.
[41] Crouhy ve Diğerleri, s.48-53.
[42] Levent Özkul, **ABD Sermaye Piyasalarında Yaşanan Son Gelişmeler ve ABD'de Yürürlüğe Giren 2002 Tarihli Sarbanes-Oxley Kanunu'nun Türk Sermaye Piyasası Açısından Değerlendirmesi**, Sermaye Piyasası Kurulu, Yayın No:166, Ankara:2002, s.2-8.
[43] Robert J**.** Chapman, **Simple Tools and Techniques for Enterprise Risk Management**, 2006, s.25-29.

Örneğin, bağımsız denetim hizmeti sunan firmaların aynı zamanda muhasebe kayıtlarını tutmak, muhasebe yönetim sistemini kurmak, aktüeryal hizmetler sunmak, iç denetim hizmeti sunmak gibi hizmetleri de sunmaları yasaklanmıştır. Bu maddenin bu şekilde düzenlemesinde, bağımsız denetim sektörünün zamanla asıl işi olan denetimden danışmanlık servisi sunumu gibi daha karlı iş kollarına kayması ve doğal olarak ortaya çıkan çıkar çatışması rol almıştır. İkincil olarak, ABD piyasalarında halka açılmak için bağımsız bir denetim komitesinin varlığı şart koşulmuştur. Bu komite bağımsız denetim firmasının seçiminden, firma ile ilişkilerin yürütülmesinden sorumlu ve kendine bağlı olarak çalışacak olan personelin de seçiminde geniş bir yetkiye sahiptir. Üçüncül olarak, halka açık şirketlerin genel müdür ve mali işler müdürüne şirketin açıklamış olduğu finansal tablolarda önemli sayılabilecek ölçüde herhangi bir hata, eksik gösterme ya da yanıltıcı içerikli bilgi yer almadığını şahsi imzaları ile taahhüt etmeleri zorunluluğu getirilmiştir. Mali tabloların doğruluğunu taahhüt eden yöneticiler aynı zamanda etkin bir iç kontrol sisteminin kurulmasından ve iç kontrol sisteminin etkin bir şekilde çalıştığının değerlendirilmesinden sorumludurlar[44]. Aynı zamanda üst yönetim, bağımsız denetimi gerçekleştiren denetim firmasına, firmanın iç kontrol sisteminde olan önemli zafiyetleri ve eksiklikleri bildirmekle yükümlüdür. Dördüncü, olarak halka açık şirketlerin yıllık faaliyet raporlarında iç kontrol sistemlerine ilişkin de bir rapor yayınlamaları istenmektedir. Aynı zamanda bağımsız denetim şirketi de yönetimin iç kontrol sistemine ilişkin değerlendirmesini incelemektedir.

1.4.4. Avrupa Birliği Düzenlemeleri

2004 Temmuz ayında yayımlanan Basel-II, G10 ülkelerinde faaliyet gösteren ve uluslararası bankacılık yapan finansal kurumlarda 2007 yılından itibaren uygulanmaya başlamıştır. Basel-II Avrupa Parlamentosu ve Konseyinin 14 Haziran 2006 tarihli, 2006/48 ve 2006/49 sayılı Direktifleri ile Avrupa Birliği (AB) müktesebatına dâhil edilmiş, üye ülkelerce 2007 başından itibaren geçiş süreciyle uygulanmaya başlanmış ve 2008 yılından itibaren de uygulanmaktadır. Direktif, Basel-II'nin sermaye yeterliliğine ilişkin önerileri temel alınarak oluşturulmuş olup sermaye yeterliliğini düzenleyen çerçeveyi daha kapsamlı ve riske duyarlı hale getirmekte, daha gelişmiş risk yönetim sistemleri oluşturmayı sağlamaktadır.

[44] Özkul, s.12-13.

Direktif, operasyonel riske ilişkin olarak, Basel Komitesi tarafından yapılan tanımı aynen benimseyerek, operasyonel riskin ölçülmesinde ve tahsis edilecek sermaye miktarının belirlenmesinde kullanılacak metodolojilerde esas itibariyle Basel Komitesi tarafından önerilen yaklaşımları ele alarak kullanılacak metotların kurumların risk yönetim tekniklerindeki gelişmelere paralel bir şekilde belirlenmesi gerektiğini düzenlemektedir.

Direktif'in Basel-II uzlaşısından farkı; Bunun sadece bankalarca uygulanmayıp aynı zamanda yatırım şirketleri tarafından da uygulanacak bir düzenleme olmasıdır. Bunun nedenleri arasında yatırım şirketlerinin de bankalar gibi benzer risklere maruz kalmaları, tek pazar içerisinde rekabetin kurallarının her bir kurum için eşit biçimde uygulanmasını sağlamak gerekliliği sayılabilir.

1.4.5. Basel Komitesi Kararları

Basel Komitesi (Committee on Banking Regulations and Supervisory Practices), uluslararası sermaye piyasalarında ve bankacılık sektöründe yaşanan problemler sonrasında 1974 yılı sonlarında, bankacılık işlemlerinin uluslararası piyasalarda belirli bir çerçevede düzenlenmesi ve denetimin sağlanması amacıyla "Group Ten" olarak adlandırılan ülkelerin merkez bankası yöneticileri ya da yerel bankacılık sektörünü düzenleyen regülatör kurumların temsilciler tarafından oluşturulmuştur.

Basel Komitesinin üyeleri; Amerika Birleşik Devletleri, Arjantin, Brezilya, Kanada, Meksika, Avustralya, Belçika, Fransa, Almanya, İtalya, Lüksemburg, Hollanda, İspanya, İsveç, İsviçre, Birleşik Krallık (İngiltere, Galler, İskoçya, Kuzey İrlanda), Çin, Hong Kong SAR, Hindistan, Endonezya, Japonya, Güney Kore, Singapur, Rusya, Suudi Arabistan, Güney Afrika Cumhuriyeti ve Türkiye olmak üzere toplam 27 ülkeden oluşmakta olup Komitenin başkanlığını Hollanda Merkez Bankası Başkanı Nout Weelink, genel sekreterliğini ise Stefan Walter yürütmektedir[45].

Komitenin sekreteryası İsviçre'nin Basel kentinde bulunan "BIS: The Bank for International Settlements" (Uluslararası Takas Bankası) tarafından yürütülmekte olup burada görev alanların önemli bir kısmını Basel Komitesinin üyesi olan ülkelerin ilgili

[45] http://www.bis.org/bcbs/index.htm (27 Haziran 2009)

kurumlarından dönemsel olarak görevlendirilen ilgililer oluşturmaktadır. Komite belirli periyotlarda İsviçre'nin Basel kentinde bulunan BIS'te toplanmaktadır.

Komitenin temel amacı, üye ülkelerin özellikle bankacılık sektörünün istikrarlı, güvenilir ve sağlam bir şekilde faaliyetlerini sürdürebilmesini teminen öne çıkan konuların anlaşılmasını ve sektörel regülasyonun kalitesinin arttırılmasına yönelik ortak çalışmalar yapmaktır. Böylelikle, ulusal denetim ve gözetim kurumları arasında bilgi ve tecrübe paylaşımı sağlanıp, ortak bir anlayışın gelişmesi ve bankaların değişik ülkelerde farklı düzenlemelerle karşılaşmaması hedeflenmektedir. Komite resmi olarak uluslararası bir bankacılık otoritesi olmadığı için formal bir yaptırım mekanizmasına sahip olmasa da, aldığı karar ve tavsiyelerin gücü, IMF ve Dünya Bankası gibi kuruluşların çalışmalarında yapılan söz konusu düzenlemeleri desteklemeleri[46] , uluslararası bankacılık faaliyetlerinde bu standartları uygulayan bankaların tercih edilmesi, Komiteye üye olan ülkelerden ve AB'nin tavsiye edilen kararları kısa zamanda müktesebatına dahil etmesinden ileri gelmektedir[47].

Komitenin sermaye yeterliliği konusundaki çalışmalarının yanında bankacılık operasyonlarından kaynaklanan risklerin yönetilmesi, karapara aklama, muhasebe uygulamaları ve yaklaşımları ve denetim konularında da çeşitli çalışmalar gerçekleştirmekte ve yayımlamaktadır. Örneğin, 1997 yılında "Etkin Bankacılık Denetimi için Temel İlkeler" (Core Principles for Effective Banking Supervison) setini yayınlamıştır. Bu ilkeler, ülkelerin bankacılık alanında denetim, gözetim ve düzenleme çerçevelerinin uluslararası standartlara uygunluğunun ölçülmesinde temel alınan referansa dönüşmüştür.

1.4.5.1. Basel –I

Basel Komitesi, 1970'lerin sonlarında üçüncü dünya ülkelerinin borç çevirim sorunlarından dolayı uluslararası bankaların sermaye yeterlilik rasyolarının kötüleşmeye başlaması üzerine konuyla ilgili olarak çalışmaya başlamıştır[48]. Komite 1975 yılından

[46] M.Hasan Eken, "Basel II ve Risk Yönetimi", http://www.tkyd.org/files/downloads/mehmet_hasan_eken_basel_ii.pdf (20 Şubat 2009), s.1.
[47] M.Ayhan Altıntaş, **Bankacılıkta Risk Yönetimi ve Sermaye Yeterliliği**, Ankara:Turhan Kitabevi, 2006 s.59.
[48] The Banker's Guide to The Basel-II Framework, The Banking Association of South Africa, 2005, http://www.standardbank.co.za/SB_FILES/BGPsite_2008/The_Bankers_Guide_to_Basel_II.pdf (6 Mart 2007), s.1-2.

itibaren yaptığı çalışmaları yayımlamaya başlamıştır. İlk yayımlanan çalışmalar "sermaye yeterliliği" ile ilgilidir. 1990'lı yıllardan itibaren de Komite bankacılık faaliyetlerinden kaynaklanan risklerin yönetilmesine, kara paranın aklanmasının önlenmesine, muhasebe ve denetim konularına ilişkin de değişik çalışmalar yapmış ve yayımlamış olmakla beraber Komitenin esas misyonunun uluslararası finans piyasalarında güven ve istikrarın sağlanmasına yönelik çalışmalar olduğu aşikardır.

Komite 1988 yılında Basel-I olarak bilinen "International Convergence of Capital Measurement and Capital Standards"ı yayınlamış ve söz konusu Uzlaşı 1992 yılında uygulanmaya başlamıştır.

Basel-I ile bir sermaye yeterliliği ölçüm yaklaşımı oluşturularak, bankaların kredi riski taşıyan faaliyetleri ile ellerindeki sermaye arasında bağlantı kurulması amaçlanmıştır.[49] Buna göre, bankların mali tablolarında yer alan risk ağırlıklı varlıklarına istinaden en az % 8 oranında sermayeye sahip olması öngörülmekteydi. Metinde risk ağrılıklı varlıklar kredi verilen karşı tarafa ve kredi teminatına bağlı olarak Tablo 2'de görüldüğü üzere 4 ana kategoriye ayrılmıştır.

Tablo 2: Basel-I: Risk Kategorileri ve Varlık Türleri

Risk Ağırlığı	Varlık Türleri
%0	OECD üyesi ülkelerin Hazine ve Merkez Bankaların kullandırılan krediler
%20	Çok taraflı kalkınma bankları ve OECD üyesi ülkelerin bankalarına kullandırılan krediler
%50	İpotek karşılığı kullandırılan krediler
%100	OECD üyesi olmayan ülkelerin Hazine, Merkez Bankaları ve ticari banklarına kullandırılan krediler ve özel sektör kuruluşlarına kullandırılan krediler

Kaynak: International Convergence Of Capital Measurement And Capital Standards, 1988 s.21-23

1996 yılında yayınlanan yeni metinle (Overview of the Amendment to the Capital Accord to Incorporate Market Risks) piyasa riski, bankaların bilanço içi ya da dışı pozisyonlarında piyasa fiyatlarındaki muhtemel görülen değişiklikler nedeniyle karşılaşabileceği kayıp riski olarak tanımlanmış, bankalara piyasa riski ölçümünde standart

[49] Bolgün ve Akçay, s.85.

ve içsel modellerin kullanılması yaklaşımı olmak üzere iki farklı yaklaşımdan birini tercih etme imkanı verilmiş ve öz kaynak hesabına 3. kuşak sermaye de ilave edilmiştir[50].

Basel-I, öncelikli olarak G-10 üyesi ülkelerde faaliyet gösteren ve uluslararası düzeyde operasyonları olan bankaların sermaye yeterliliğine ilişkin olarak hazırlanmış olsa da belirli bir süre sonra tüm dünyada 100'den fazla ülkede bankaların sermaye yeterliliğine ilişkin bir düzenleme olarak kabul edilmiştir. Diğer taraftan, Basel-I kapsamında yer alan risk ağırlıklandırması bazı tartışmalara da sebep olmuştur. Örneğin, Tablo 2'de de gösterildiği gibi OECD üyesi ülkelere verilen krediler risksiz olarak değerlendirilirken üye olmayan ülkelere verilen krediler %100 olarak değerlendirilmiştir ve Komite OECD üyeleri arasındaki risklilik değerlendirmesi yapmamış ve risk değerliliği açısından her üye ülkeyi aynı kabul etmiştir. Diğer taraftan kredi riskini ölçmeye dönük yöntemin çok basit olması, sermaye yeterlilik rasyosu için belirlenen kritik değerin %8 gibi esnek olmayan bir oran olması, uygulamanın piyasalarda sunulan hizmetler ve kurumların alt yapılarının gelişmişliğinden bağımsız olarak tüm finansal kurumlara aynı şekilde bakması da yeterince hassas bir risk ölçümünün olmadığı yönündeki görüşleri kuvvetlendirmiştir[51].

Her ne kadar Basel-I kriterleri genel olarak dünyadaki bir çok finans kurumu ve denetim otoritesi açısından kabul edilmiş ve birçok kurumun sermaye oranlarını önemli derecede artmış olsa da finans sektöründe gelişen yeni ürünler, riskin farklı kaynaklardan doğması gibi nedenlerden ötürü Basel-I çerçevesinde hesaplanan sermaye yeterliliğinin mali kurumun riskini en iyi bir şekilde yansıtmadığı sonucuna ulaşılmıştır. Zira, kredi riskinin hesaplanmasına yönelik eleştiriler yanında tavsiyeler setinin piyasa riski daha sonrasında eklenmesine karşın operasyonel riskleri sermaye yeterliliğinde hesaplamaya dahil edilmemesi bu konudaki eksikliğin kaynağını oluşturmaktaydı. Bu kapsam dahilinde, Komite Basel-I in eleştirilen yönlerini de göz önüne alarak yeni ve daha kapsamlı bir Uzlaşı setini Basel-II'yi oluşturmuştur.

[50] BCBS, "Overview of the Amendment to the Capital Accord to Incorporate Market Risks", 1996, http://www.bis.org/publ/bcbs23.htm (13 Nisan 2007), s.1-2,
[51] Altıntaş, s.62-63.

1.4.5.2. Basel –II

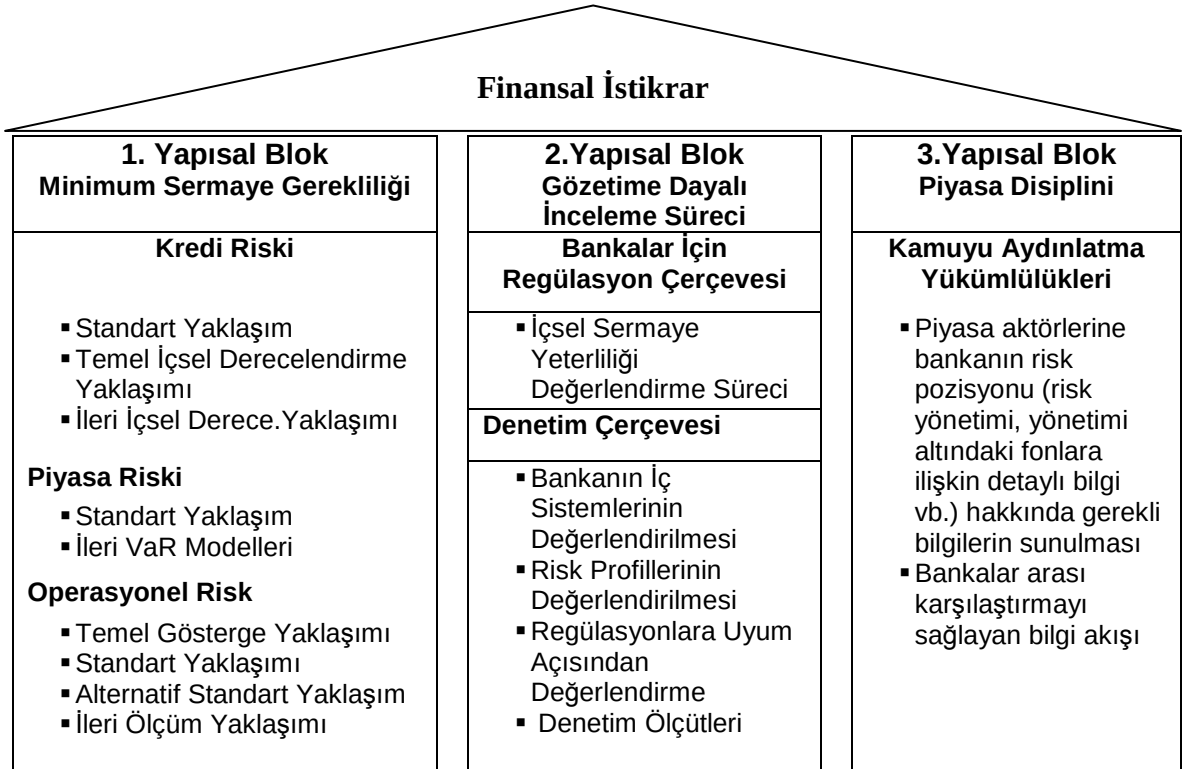
Komite, Basel-I kapsamındaki mevcut düzenlemelerin bankaların sermaye düzeyleri ile taşıdıkları riskler arasındaki bağlantıyı tam ve doğru bir şekilde kuramaması, piyasa disiplinini gözardı etmesi ve finansal piyasalarda görülen gelişmeler nedeniyle[52] yeni bir uzlaşı seti oluşturmak için 1999 yılında çalışmalara başlamış ve Haziran 2004'te Basel-II olarak bilinen "International Convergence of Capital Measurement and Capital Standards"ı yayımlamıştır.

Basel-II düzenlemesinin göze çarpan özellikleri; onun sermaye yeterliliği hesabında daha karmaşık bir ölçüm çerçevesi içermesi, sadece bir sermaye yeterlilik düzenlemesi olmayıp aynı zamanda finansal organizasyonlara kurumsal yönetim ve şeffaflık sağlayan bir risk yönetimi yapısı getirmesi, bankanın ölçeği ve büyüklüğüne bağlı olarak üç tip risk ölçüm yaklaşımı sunması ve bu yaklaşımların hangisinin benimseneceğine daha esnek bir yapıda kurumun karar vermesine olanak sağlaması, kredi ve piyasa risklerinin aksine operasyonel risk üzerine yoğunlaşması, riske daha duyarlı bir yaklaşım olması olarak sıralanabilir[53]. Ama diğer taraftan ise Basel-II kapsamında ölçülen riskler bütünüyle sermaye yeterliliğinin hesaplanması perspektifinden olması dolayısıyla risklerin yönetilmesine ilişkin kapsamlı bir hedef göstermemektedir[54].

Basel-I düzenlemesi tek tip risk ölçümüne odaklı iken, yeni düzenleme bankalara dahili metotlar kullanarak içsel ölçümler yapabilmelerine, kendi risk yönetim metodolojilerini geliştirebilmelerinin yanı sıra denetimlere ve piyasa disiplinine dayalı bir yapı önermektedir. Basel-II olarak adlandırılan yeni uzlaşı seti eskisine göre daha kapsamlı risk tanımları, ölçüm yöntemleri ve risk değerleme hassasiyetine sahiptir. Basel-I düzenlemesinin dayandığı tek yapısal blok sermaye gereği veya sermaye yeterliliği iken Basel-II düzenlemesi üç yapısal blok üzerine kurulmuş olup Basel-II'nin ilişkisel mimarisi Şekil 1'de gösterilmektedir.

[52] Eken, s.2.
[53] Moosa, s.39-40.
[54] Eken,s.3.

Şekil 1: Basel-II'nin Üç Yapısal Bloğu



Kaynak: http://www.fma.gv.at/cms/basel2/EN/einzel.html?channel=CH0272 (25 Mayıs 2008)

Birinci yapısal blok bankaların gözetim sermayesi (regulatory capital) hesaplamalarına kredi ve piyasa risklerinin yanısıra operasyonel riski de dahil eden *"Minimum Sermaye Gerekliliği"*dir. İkinci yapısal blok ilgili bankanın etkin bir risk yönetimine sahip olmalarına ilişkin olarak denetim otoritesinin banka hakkında detaylı bir takım inceleme ve değerlendirmelerde bulunması ile ilgili olan "*Gözetime Dayalı inceleme Süreci*"dir. Üçüncü yapısal blok ise bankaların riskleri, risk yönetim sistemleri ve sermaye yeterlilikleri konularında daha şeffaf bir yönetim anlayışıyla kamunun bilgilendirilme sürecini kapsayan *"Piyasa Disiplini"*dir[55].

Birinci yapısal bloğu oluşturan *"Minimum Sermaye Gerekliliği"* altında, Uzlaşıda bankaların karşı karşıya bulundukları en önemli riskler olarak belirtilen kredi riski, piyasa riski ve operasyonel risk için asgari tutarda sermaye bulundurulması gerektiği ifade

[55] Carol Alexander, **Operational Risk: Regulation, Analysis and Management,** London ; New York:Financial Times Prentice Hall, 2003, s.3-4.

edilmiştir. Dolayısıyla, Basel-II bankaların maruz kaldığı riskleri; kredi riski, piyasa riski ve operasyonel risk olarak üç ana gruba ayırmıştır. Komite operasyonel riski *"yetersiz veya başarısız iç süreçleri, personel, sistemler ve dışsal olaylar sonucu ortaya çıkan kayıp"* şeklinde tanımlamakta ve bu riski ölçebilecek bir yapı öngörmektedir. Basel Komitesinin tanımlamasında operasyonel risk kapsamına "yasal risk" dahil edilmesine karşın "itibar" ve "strateji riski" dahil edilmemiştir[56]. Dolayısıyla Uzlaşı bankaların sermaye yeterliği hesaplanmasında aşağıda yer alan formülü öngörmektedir:

$$SermayeYeterliliği = \frac{(Tier1)+(Tier2)+(Tier3)}{RiskAğırlıklıAktifler(KRET+PRET+ORET)} \geq \%8 \qquad \textbf{(1)}$$

***Tier*1** : Ana Sermaye
***Tier*2** : Katkı Sermaye
***Tier*3** : Üçüncü Kuşak Sermaye
KRET : Kredi Riskine Esas Tutar
PRET : Piyasa Riskine Esas Tutar
ORET : Operasyonel Riske Esas Tutar

Yukarıdaki formülün payını oluşturan Tier 1-2 ve 3 olarak Uzlaşı'da ifade edilen "Gözetim Sermayesi" (Regulatory Capital) tanımı, Basel-I de ifade edilen tanımı esas almakla beraber kredi riskinin hesaplamasında standart yaklaşım veya içsel derecelendirme metodunun kullanılmasına bağlı olarak bazı eklemeler veya indirimlerin yapılmasını öngörmektedir[57].

Basel-II, sermaye yükümlülüğünün hesaplanmasında gerekli olan operasyonel riske esas tutarın belirlenmesi sürecinde temel gösterge yaklaşımı ve standart yaklaşımda olduğu gibi ileri ölçüm yaklaşımları için belirli bir hesaplama modelinin kullanılmasını öngörmemiştir. Böylelikle, ileri ölçüm yöntemini kullanacak olan kurumların farklı risk ölçüm yöntemlerini geliştirebilmeleri sağlanmış olacaktır. Çünkü, operasyonel risklerin çok yönlü

[56] BCBS, "International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version", 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008), s.144.
[57] BCBS, "International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version", 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008), s.12.

ve diğer risklerden farklı yönlerinin olduğundan hareketle, riski daha duyarlı şekilde ölçebilecek güvenilir birçok farklı yöntemin geliştirilmesini teşvik etmek amacıyla herhangi bir ölçüm yöntemi isim olarak zikredilmemektedir[58].

1.4.5.3. Basel Komitesinin Operasyonel Risk Yönetim Prensipleri

Basel Bankacılık Komitesi etkin bir operasyonel risk yönetimi için 10 temel prensip benimsenmiştir[59].

Bu prensipler;

1. Bankanın maruz bulunduğu önemli operasyonel risklerin yönetim kurulu tarafından bilinmesi ve operasyonel risk yönetim stratejisinin yönetim kurulu tarafından onaylanması,
2. Yönetim kurulunca onaylanan risk yönetim stratejisinin uygulanması ile ilgili olarak üst düzey yönetimin görevlendirilmesi,
3. Bankadaki her seviyedeki personelin ve her birimin operasyonel riskler ile ilgili sorumluluğunun açıkça tarif edilmesi,
4. Etkin bir risk yönetim sisteminin oluşturulmasında banka organizasyonu içindeki bilgi akışının anahtar rol oynadığı, banka içindeki iletişim sisteminin risk yönetim kültürünün etkin bir aracı olarak dizayn edilmesi gerekliliği, bilgilendirme ve rapor akışlarının üst düzey yönetimin operasyonel risk yönetim sisteminin etkinliğini izleme imkanı vermesi,
5. Bankaların tüm ürün, faaliyet, süreç ve sistemleri ile ilgili operasyonel risklerin belirlenmesi, yeni ürün, faaliyet, süreç ve sistemler ile ilgili olarak bunların işletime veya uygulamaya alınmadan risk değerlendirmelerinin yapılması,
6. Bankaların operasyonel risklerinin ölçebilmelerini temin edecek yeterli sistemlerinin bulunması, bankaların tüm temel faaliyet kolları itibariyle operasyonel risk gerçekleşmelerini, risk gerçekleşmesi dolayısıyla uğradıkları kayıpları sürekli olarak izleyebilecek bir sistem oluşturmaları,
7. Bankaların operasyonel risklerini kontrol edebilecek veya azaltabilecek politika, süreç ve sistemlere sahip olmaları, bankaların alternatif risk limitleri ile uygulanan risk önleme yöntemlerinin fayda ve maliyetlerini bankanın genel risk profili kapsamında değerlendirilerek en uygun strateji ve limitlerin ihdası,

[58] Murat Mazıbaş, "Operasyonel Riske Bazel Yaklaşımı: Üç Yapısal Blok Çerçevesinde Bir Değerlendirme", **BDDK Araştırma Raporları**, 2005/1, s.8.
[59] BCBS, "Sound Practices For the Management and Supervision of Operational Risk", December 2001.

8. Denetçilerin banka genel risk yönetimi çerçevesinde operasyonel riskleri de tanımlayan, ölçebilen, izleyebilen ve kontrol edebilen etkin bir operasyonel risk yönetim sisteminin mevcudiyetini sorgulamaları,

9. Risk yönetimi kapsamında etkin bir iletişim ve raporlama sisteminin bulunup bulunmadığını ve risk yönetim politika, prosedür, süreç ve uygulamalarının düzenli olarak bağımsız bir değerlendirmeye tabi tutulup tutulmadığını kontrol etmeleri,

10. Kamuyu aydınlatma kapsamında bankaların tüm piyasa katılımcıları ve ilgili tüm kişi ve kuruluşları operasyonel risk yönetimi kalitesi ve risk gerçekleşmeleri konusunda yeterli düzeyde bilgilendirilmesi önerilerini içermektedir.

Komitenin belirlemiş olduğu prensipler değerlendirildiğinde, operasyonel risklerin yönetiminde etkin bir iç kontrol sisteminin mevcudiyeti şartının, arandığı görülmektedir. BDDK tarafından iç denetim ve risk yönetim sürecine ilişkin olarak yapılan düzenlemelerde, bağımsız bir iç kontrol merkezi/birimi kurulması zorunlu tutulmuş ve bu birimin sürekli bir kontrol faaliyeti ile görevlendirilmesi gereği bildirilmiştir. BDDK ile Basel Bankacılık Komitesinin iç kontrol süreci ve iç kontrol sistemi ile ilgili tanımlamaları büyük ölçüde benzerlik arz etmesine rağmen, BDDK'nın iç kontrol birimi/merkezine yüklediği geniş çerçeveli görev ve sorumluluklar konusunda tartışmalar bulunmaktadır[60]. Bankacılık sisteminde yapılan ve tepki nitelikli düzenlemeler sonucunda, bankalarda, iç kontrol merkezi, risk yönetim grubu ve teftiş kurulundan oluşan üçlü bir iç denetim ve risk yönetimi yapılanması oluşturulmuştur.

1.4.5.4. Operasyonel Risk Ölçüm Yaklaşımları

Basel-II bankaların, sermaye yeterliliği hesabında operasyonel riske esas tutarın hesaplanabilmesi için dört farklı yaklaşım önermiştir. Aşağıda belirtilen her bir yaklaşım bir öncekine göre daha kapsamlı, daha gelişmiş ve risk duyarlılığı daha yüksek uygulamalar içermektedir.

- Temel Gösterge Yaklaşımı
- Standart Yaklaşım
- Alternatif Standart Yaklaşım

[60] Yavuz Salih Tanju, "İç Kontrol Fonksiyonun Bileşenleri, İç Kontrol Merkezi Teftişten Farklı Bir Mekanizmadır"**,** TBB, **Bankacılar Dergisi**, Sayı.42, 2002, s.39-55.

- Gelişmiş Ölçüm Yaklaşımları

Bankaların bir sonraki ölçüm yaklaşımını kullanabilmeleri için belirli bir takım niteliksel ölçütleri karşılayabiliyor olmaları gerekmektedir. Bankanın daha kapsamlı bir operasyonel risk ölçüm yaklaşımını uygulamak için ulusal düzenleyici ve denetleyici otoritesinden onay alması gerekmektedir. Bankanın operasyonel risk ölçümüne ilişkin olarak gelişmiş ölçüm yaklaşımını uyguladıktan sonra daha sonraki aşamada daha basit bir yönteme geçmesi mümkün değildir. Eğer banka onay aldıktan sonra onay almasına temel teşkil eden niteliksel standartlardan geriye düşmüşse yine aynı standartları karşılayana kadar daha basit bir ölçme yaklaşımını kullanmasına izin verilebilir. Uzlaşı, ayrıca bankalara belirli operasyonları için Temel Gösterge Yaklaşımı" veya "Standart Yaklaşımı", diğer bazı operasyonları için de "Gelişmiş Yaklaşımları" kullanabilmelerine belirli kriterleri karşılamaları durumunda imkan sağlamaktadır[61].

Uzlaşı, operasyonel riske ilişkin olarak bankalarca ayrılması gereken sermaye miktarının, bankaların operasyonel riskin ölçümüne ilişkin daha kapsamlı ve riske duyarlı yöntemler izlemesine bağlı olarak daha az miktarda sermaye tutmalarına olanak sağlayacağını öngörmektedir. Ancak, pratik olarak daha gelişmiş bir operasyonel risk ölçüm metodolojisi izleyen bir bankanın daha basit yaklaşımları uygulaması neticesinde daha fazla sermaye tutması gerekliliği de ortaya çıkabilir[62].

1.4.5.4.1. Temel Gösterge Yaklaşımı (Basic Indicator Approach)

Temel gösterge yaklaşımında, bankanın son üç yıl itibariyle gerçekleşen yıl sonu brüt gelir tutarlarının %15'inin ortalamasının 12.5 ile çarpılması suretiyle bulunacak değer, operasyonel riske esas tutar olarak dikkate alınır.

Bu tanımda yer alan brüt gelir; net ücret ve komisyon gelirlerinin, temettü gelirlerinin, ticari kâr/zararın (net) ve diğer faaliyet gelirlerinin eklenmesi, satılmaya hazır ve vadeye kadar elde tutulacak menkul kıymetler hesaplarında izlenen menkul kıymetlerin satışından kaynaklanan kâr/zarar ile olağanüstü gelirler (iştirak ve bağlı ortaklık hisseleri ile

[61] BCBS, "International Convergence of Capital Markets and Capital Standards, A Revised Framework Comprehensive Version", 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008), s.144.
[62] T.İş Bankası Risk Yönetim Müdürlüğü, **Bankacılıkta Yeni Sermaye Yeterliliği Düzenlemeleri: Basel-II,** T.İş Bankası Yayın No:78, 2004, s.43-44.

gayrimenkul satış kazançları dahil) ve sigortadan tazmin edilen tutarların[63] düşülmesi suretiyle hesaplanmaktadır.

Böylelikle operasyonel riske esas olan tutar, bankanın brüt gelirinin yaklaşık olarak iki katına denk gelen bir tutar olacaktır ve ayrılması gereken sermaye de bu tutar üzerinden hesaplanacaktır. "Temel Gösterge Yaklaşımı" bağlamında operasyonel risk esas olan tutar aşağıdaki formül vasıtasıyla hesaplanacaktır:

$$K_{TGY} = \left[\sum (GI_{1..n} X \alpha) / n\right] \qquad \textbf{(2)}$$

K_{TGY}= Temel gösterge yaklaşımına göre bulundurulacak sermaye miktarı.

GI= Son üç yılın yıllık pozitif brüt gelir toplamı.

n= Son üç yıl içinde brüt gelirin pozitif olduğu yılların sayısı.

α= Komitenin tespit ettiği sabit oran (mevcut oran: %15).

Kaynak: BCBS, International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version, 2006, s.137.

Bu yöntemin kullanılmasındaki mantık, bir bankanın gelir elde etmek için faaliyette bulunduğu ve gelir üretimi ile operasyonel riske sebep olan faaliyetler arasında pozitif bir korelasyon olduğudur. Diğer taraftan ise, bankaların operasyonel risk düzeylerinin sahip oldukları içsel kontrol sistemlerinin kalitesinden bağımsız olarak doğrudan ve orantısal olarak sadece önceden belirlenmiş tek bir orana göre hesaplanmasına dönük de eleştiriler vardır. Eleştirilerin temel noktası, bankalardaki risk düzeyinin bu şekilde basitçe ve tüm kurumları içsel olarak benzer gören bir biçimde ölçülmesi risk ölçümünün kurumun içsel kontrol sistemlerinin kalitesine karşı duyarsız olarak bir ölçüm yapacağıdır[64]. Zaten çalışmanın uygulama kısmında Uzlaşının sermaye yeterliliği ölçümüne ilişkin önerdiği yaklaşımlara bir öneri olarak getirilen "Operasyonel Risk Yönetimi Olgunluk Seviyesi" endeksi hesaplanacak ve bu endekse bağlı olarak belirlenen bir katsayının sermaye yükümlülük hesaplamasında dikkate alınması önerilmiştir.

[63] BCBS, "International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version", 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008), s.145.
[64] Candan ve Özün, s.234.

Her ne kadar bu yöntemin basitliği ve riski etkin bir şekilde ölçemeyeceği yönündeki eleştiriler geçerli olsa da Komite operasyonel riske yönelik ölçüm yaklaşımlarını basitten daha karmaşığa göre düzenlemiş olup, gerekli alt yapısı olan ve risklilik düzeyini daha net bir şekilde ölçmek isteyen özellikle uluslararası bankacılık faaliyetlerinde bulunan büyük ölçekli bankaların daha gelişmiş yöntemleri kullanmasını beklemektedir. Bu bağlamda, yeterli kaynağı ve alt yapısı olmayan ve genel olarak da yerel ölçekte faaliyetlerde bulunan bankaların ise basit şekilde temel gösterge yaklaşımını kullanabilmesi ve Basel-II ile uyumlu olarak sermaye yeterliliğini hesaplayabilmesini teminen bu yaklaşımın "evrimsel bir sürecin" ilk basamağı olarak değerlendirilmesi gerektiği düşünülmektedir[65]. Yine, küçük ölçekli finansal kurumlar penceresinden bakıldığı zaman böyle bir formülde brüt gelirin temel referans olarak kullanılması diğer benzer referans noktalarına[66] kıyasla kötünün en iyisi olarak değerlendirilebilir[67]. Her ne kadar Komite temel yaklaşımın faaliyet alanının genişliği ve büyüklüğünden bağımsız olarak bankalar tarafından kullanılması konusunda her hangi bir ön koşul belirtmemiş olsa da yerel denetim otoritelerinin uluslararası ölçekte faaliyet gösteren kurumların bu yaklaşımı kullanmasına olanak vermeyeceğini düşünmektedir. Diğer taraftan ise bu yöntemi kullanacak olan orta ve küçük ölçekli bankaların en azından Komite tarafından 2003 yılında yayınlanan operasyonel risk yönetimine ilişkin genel prensipleri uyguluyor olmaları beklenmektedir[68].

1.4.5.4.2. Standart Yaklaşım (Standardized Approach)

"Standart Yaklaşım", farklı iş kolları için farklı göstergeler kullanılarak sermaye yeterliliğini hesaplamayı hedeflemektedir. Bu yaklaşımdaki faaliyet kolları ve faaliyetlerin

---

[65] V. Dowd, "Measurement of Operational Risk: The Basel Approach", Carol Alexander (Ed.), **Operational Risk: Regulation, Analysis and Management**, London,2003, PrenticeHall, s.40.

[66] D. Chorafas, *"Brüt gelir yerine kullanılabilecek diğer bazı referans noktaları şu şekilde sıralanmıştır: çalışan sayısı, varlıkların defter değeri, kurumun piyasa değeri, toplam mevduat,müşteri hesapların toplam sayısı, müşteri hesaplarındaki ortalama bakiye. Yine; işlem adedi, kesilen fiş sayısı, işlemlerin ortalama değeri ve standart sapması gibi yapılan işlemleri temel alarak da bazı alternatif referans noktaları belirlenebilir olsa da her biri bir şekilde brüt gelirden daha etkin bir ölçüm aracı olabileceği konusunda ikna edici gelmemektedir".*, s.146.

[67] R.A. Nash, "The Three Pillars of Operational Risk", Carol Alexander (Ed.), **Operational Risk: Regulation, Analysis and Management**, London,2003, PrenticeHall, s.5.

[68] BCBS, "Working Paper on the Regulatory Treatment of Operational Risk", 2001, http://www.bis.org/publ/bcbs_wp8.pdf?noframes=1 (23 Temmuz 2007), s.11.

detay açıklaması ile her bir faaliyet kolu için belirlenmiş olan oranlar Tablo 3'de yer almaktadır.

Tablo 3: Bankaların Ana Faaliyet Kollarına İlişkin Oranlar ve Faaliyetler

Faaliyet Kolları	Faaliyetler	Oran (%)
Kurumsal bankacılık	Sermaye piyasası araçlarının ihracına, varlıkların menkul kıymetleştirilmesine, sendikasyon kredisi kullandırımlarına ve şirket birleşme ve devralmalarına yönelik danışmanlık ve aracılık hizmetleri ve bu kapsamda edinilen ortaklık payları ile kamu kurumlarına doğrudan ya da satın alınan borçlanma senetleri aracılığıyla verilen krediler ile perakende bankacılık faaliyet kolu dışında kalan mevduat veya katılım fonu kabulü,	**18**
Alım satım	Para piyasası ve sermaye piyasası araçlarının alım ve satımı ile geri alım veya tekrar satım taahhüdü işlemleri, efektif dahil kambiyo işlemleri, kıymetli maden ile bunlara veya emtiaya dayalı sözleşmelerin alım satımı	**18**
Perakende bankacılık	Bir milyon Euro veya muadili bir para karşılığı veya daha düşük tutarda olmak üzere, gerçek veya tüzel kişilere kullandırılan her türlü nakdi ve gayrinakdi krediler ile mevduat veya katılım fonu kabulü, kredi kartlarına dayalı işlemler	**12**
Perakende aracılık	Kurumsal bankacılık dışındaki aracılık faaliyetleri	**12**
Ticari bankacılık	Bir milyon Euro veya muadili bir para veya daha fazla bir tutarda nakdi ve gayrinakdi kredi kullandırımları, faktoring, forfaiting, finansal kiralama ve dış ticaret işlemleri	**15**
Takas ve ödemeler	Fatura ödemelerine aracılık işlemleri, havale hizmetleri, takas hizmetleri	**18**
Acente hizmetleri	Sigorta acenteliği ve bireysel emeklilik aracılık hizmetleri ile kiralık kasa ve saklama faaliyetleri	**15**
Varlık yönetimi	Fon yönetimi	**12**

Kaynak: Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik (Md:16).

Standart yöntemde operasyonel riske esas tutar, yıllar itibariyle faaliyet kolları bazında bulunacak sermaye yükümlülüğü tutarları toplamının son üç yıllık ortalamasının 12.5 ile çarpılması suretiyle bulunur. Yıllar itibariyle faaliyet kolları bazında sermaye yükümlülüğü toplamı, her bir faaliyet koluna ilişkin yıllık brüt gelirin Tablo 3'de yer alan bu faaliyet kollarına karşılık gelen oranlar ile çarpılması suretiyle bulunacak değerlerin her bir yıl için ayrı ayrı toplanması suretiyle hesaplanır[69].

Bu yaklaşım çerçevesinde operasyonel riske ayrılacak sermayeyi hesaplamak için, gelir elde edilen faaliyetin Basel-II çerçevesinde belirlenen faaliyet kollarından hangisine dahil olduğunun belirlenmesi gerekmektedir.

[69] BDDK, "Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik (Md:16)".

Bu hesaplama yapılırken, herhangi bir yıla ilişkin faaliyet kolları bazında hesaplanan sermaye yükümlülüğü toplamının negatif olması halinde, yıllar itibariyle faaliyet kolları bazında bulunacak sermaye yükümlülüğü tutarları toplamının üç yıllık ortalamasının hesabında bu yıla ilişkin sermaye yükümlülüğü toplamı sıfır olarak dikkate alınır. Standart yaklaşım kapsamında yasal sermaye yükümlülüğü aşağıda formül ile hesaplanmaktadır[70]:

$$K_{SY} = \left\{ \sum_{yıl} \max \left[\sum \left(BG_{1-8} * \beta_{1-8} \right), 0 \right] \right\} / 3 \qquad \textbf{(3)}$$

K_{SY} = Standart yaklaşıma göre yasal sermaye yükümlülüğü.

BG_{1-8} = Sekiz faaliyet kolunun her biri için belirli bir yıldaki brüt gelir.

β_{1-8} = Komitece belirlenmiş olan beta katsayısı.

Kaynak: BCBS, International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version, 2006, s.140.

Bu yaklaşımın ana mantığı, bankanın her bir iş kolunun birbirinden daha farklı derecede riske maruz kaldığı ve bankanın gelir elde etmek için gerçekleştirdiği ana ve önemli faaliyetlerin, farklı risk katsayıları ile ağırlıklandırarak toplam risk duyarlılığının daha sağlıklı ölçülebileceğidir. Örneğin, büyük ölçekli bir bankada yatırım bankacılığı bölümünün varlık yönetimi bölümüne göre daha fazla riske maruz kalma olasılığı olduğu genel olarak kabul edilmektedir[71].

Bankanın gelir temin etmek için yürüttüğü faaliyetlerin farklı risk ağırlıklarına tabi tutulmasıyla risk duyarlılığı artmış olsa da risk duyarlılığındaki artışın sınırlı olduğu da doğrudur. Temel gösterge yaklaşıma yönelik eleştiriler bu yaklaşım için de ileri sürülmektedir, çünkü standart yaklaşım da operasyonel risk ve brüt gelir arasındaki ilişkiden hareketle sermaye yeterliliğini belirlemeyi öngörmektedir. Diğer taraftan ise, bankaların standart yaklaşımı kullanabilmeleri için, Basel-II düzenlemeleri kapsamında, belirlenmiş olan bazı koşulları sağlamış olmaları gereklidir ki bu da bankanın operasyonel riskin yönetimi konusunda belirli bir aşama kaydettiği anlamına gelmektedir. Burada bahsedilen ön koşullar şunlardır[72]:

[70] Candan ve Özün, s.236.
[71] Moosa, s.51.
[72] Moosa, s.52.

-Bankanın yönetim kurulunun ve(ya) üst düzey yönetiminin, operasyonel risk düzenlemesinin gözetimi konusunda etkin rol oynaması gerekmektedir.

-Bankanın operasyonel risk yönetim sistemi kavramsal olarak güçlü olmalı ve tüm kurum çapında uygulanmalıdır.

-Kontrol ve denetim alanlarının yanı sıra, temel faaliyet kollarında da bu yaklaşımın uygulanabilmesini sağlamak üzere yeterli kaynak bulundurulmalıdır.

Yukarıda belirtilmiş olan koşullar ileri ölçüm yöntemlerini kullanacak olan kurumlar içinde geçerlidir. Yine uluslararası bankaların standart yaklaşımı kullanabilmeleri için de uymaları gereken ek kriterler mevcuttur[73]:

Bu ölçekteki bir bankanın, operasyonel risklerin belirlenmesi, değerlendirilmesi, kontrol edilmesi, raporlanması ve azaltılması, operasyonel risk politikalarının oluşturulması, operasyonel risk değerlendirme metodolojisinin tasarlanması ve uygulanmaya konulmasından sorumlu ayrı bir fonksiyonu bulunmalıdır. Operasyonel risk değerlendirme sistemin bir parçası olarak faaliyet kolları bazında kayıp verilerinin kaydedilmesi, bu verilerin risk raporlamasında ve risk analizinde önemli rol oynaması sağlanmalıdır. Yönetim kurulu, üst düzey yönetim ve ilgili birimlere operasyonel risk verilerinin düzenli olarak raporlanması gerekmektedir. Operasyonel risk yönetim sistemin ayrıntılı bir şekilde yazılı hale getirilmiş olması şarttır. Operasyonel risk yönetimi süreçlerinin ve değerlendirme sisteminin düzenli olarak bağımsız iç denetimden geçmesi gerekmektedir. Bankanın operasyonel risk değerlendirme sistemi bağımsız dış denetçiler veya denetim otoritesi tarafından süzenli olarak gözden geçirilmelidir.

Bu bağlamda, operasyonel riske esas tutarın hesaplanmasında standart yaklaşım da temel gösterge yaklaşımı gibi brüt geliri esas alıyor olsa da, yöntemin risk duyarlılığı açısından temel gösterge yaklaşımına göre daha ileri bir yöntem olduğu söylenebilir. Çünkü, bankaların ve özellikle de uluslararası bankacılık gerçekleştiren kurumların bu yaklaşımı uygulayabilmeleri için yerine getirmesi gereken unsurlar ve önkoşullar kurumun

[73] BCBS, “International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version”, 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008), s.148-149.

operasyonel riskin ölçümü ve yönetimi konusunda oldukça iyi bir mesafe kat ettiği anlamındadır.

1.4.5.4.3. Alternatif Standart Yaklaşım

Standart yaklaşımın bir alt kolu olan " Alternatif Standart Yaklaşım" da ticari ve perakende (bireysel) bankacılık faaliyet kollarında üretilen faaliyet geliri yerine, bu iş kolları dahilinde kullandırılan kredi tutarının sabit bir değer (0.035) ile çarpılması neticesinde elde edilecek risk tutarı (Gösterge) sermaye yeterliliği hesabında dikkate alınmaktadır.

Standart yaklaşıma ilişkin daha basit bir uygulamayı tercih etmek isteyen kurumlar ise, daha basit olarak perakende ve ticari kredilerini tek bir iş kolu olarak değerlendirip toplam olarak elde ettiği kredi portföyünü tek bir katsayı (% 15) ile çarparak ve diğer geriye kalan iş kollarından elde ettiği brüt geliri de %18 kat sayısı ile çarparak (Tablo 4'deki 2.seçenek sütunu) gerekli sermaye tutarını bulabilirler.[74]

Tablo 4: Alternatif Standart Yaklaşım

		Beta Faktörü(β)	
Faaliyet Kolları	**Gösterge**	**1.Seçenek**	**2.Seçenek**
Kurumsal bankacılık	BG_1	18%	18%
Alım satım	BG_2	18%	18%
Perakende bankacılık	(T.Kredi *0.035)	12%	15%
Perakende aracılık	BG_3	12%	18%
Ticari bankacılık	(T.Kredi *0.035)	15%	15%
Takas ve ödemeler	BG_4	18%	18%
Acente hizmetleri	BG_5	15%	18%
Varlık Yönetimi	BG_6	12%	18%

Kaynak: Evren Bolgün ve Barış Akçay, **"Risk Yönetimi Gelişmekte Olan Türk Finans Piyasasında Entegre Risk Ölçüm ve Yönetim Uygulamaları",** 2.baskı, İstanbul: Scala Yayıncılık, Haziran 2005, s.624.

BG_1 BG_8: *Son 3 yılın ortalama brüt geliri.*

[74] BCBS, "International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version", 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008), s.146.

Bir bankanın standart yaklaşımı kullanabilmesi için yerine getirmesi gereken ön koşullar standart yaklaşımda yerine getirmesi gerekenler ile aynı paralelde olmasına karşın tek bir nokta yönünden farklılık arz etmektedir: Söz konusu kritere göre, alternatif standart yaklaşımı kullanmak isteyen bir bankanın toplam gelirlerinin %90'ının perakende ve ticari bankacılık iş kollarından yaratılıyor olması ve bu durumun bağımsız denetim raporu ile belgelendirilmesi gerekmektedir.[75] Ayrıca, banka, perakende ve ticari bankacılık faaliyetlerinin önemli bir kısmın yüksek temerrüt olasılığına sahip kredilere ilişkin olduğunu denetim otoritesine kanıtlanmalıdır[76].

1.4.5.4.4. Gelişmiş Ölçüm Yaklaşımları

Operasyonel risklerin finansal tablolarda gerçekleşen bazı dönem rakamlarına referansla hesaplanmasına dönük bir yaklaşım tarzı yerine gerçek anlamda sayısallaştırılarak ölçümünün gerçekleştirildiği ve bu ölçüm sonuçlarına göre de operasyonel riske esas tutarın belirlendiği ve asgari sermaye tahsisinin yapıldığı yöntemler "İleri Ölçüm Yaklaşımları (İÖY)" altında toplanmaktadır. Basel-II, piyasa riskine esas tutarı hesaplarken kullanılan ve genel kabul görmüş olan "riske maruz değer" (RMD) ne benzer bir şekilde operasyonel riskin ölçümünde üzerinde uzlaşılmış olan ve genel kabul görmüş bir yöntem öne çıkarılmamıştır. Yukarıda da bahsedildiği gibi Basel-II operasyonel riskin çok yönlü olmasından dolayı ve kurumlarca geliştirilecek yöntemlerin farklı unsur,detay ve yaklaşım tarzlarını geliştirebileceğinden hareketle operasyonel risk ölçümünde kullanılması için spesifik bir yöntem belirlememiştir.

Temel gösterge yaklaşımı, standart yaklaşım ve alternatif standart yaklaşım operasyonel risk için ayrılması gereken sermaye miktarını brüt gelirin, önerilen katsayılar ile çarpılması sonucunda elde edilmesini öngörmektedir. Bu yaklaşımlar, sadece bankanın mali tablolarından hareket ettikleri için bankanın maruz kaldığı operasyonel riskin niteliği ve risk noktaları hakkında yeterince bilgi sağlamamaktadır. İleri ölçüm yaklaşımları ise, sadece bankanın kendine özgü ve belirli bir zaman dilimini kapsayan kayıp verilerinin olması durumunda uygulanabilecek bir yöntem olduğu için bankanın maruz kaldığı operasyonel riskin niteliğini ve sınıflandırılmış miktarını ortaya koymaktadır.

[75] BDDK, "Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik (Md:17)".
[76] Candan ve Özün, s.239.

Komite, bankaları iç verilerini de kullanarak kendi ileri ölçüm sistemlerini geliştirmelerini ve bu doğrultuda gerekli olan sermaye tahsisini yapmaları yönünde teşvik etmektedir[77]. İleri ölçüm yaklaşımının tercih edilmesine bağlı olarak sermaye yeterliliği oranının daha az gerçekleşeceği yönündeki beklentilerin yanı sıra bu yaklaşımın bankalara esneklik ve risk yönetimi konusunda da etkin bir disiplin kazandıracağı beklenmektedir. Çünkü bu yaklaşım çerçevesinde bankalar, operasyonel risk ölçümü konusunda kendi özgün yöntemlerini geliştirecekler, sektörel ortalamalara göre geliştirilmiş oranlar ile diğer yaklaşımlara kıyasla kendi kayıp veri tabanlarını tutacaklar, birçok risk faktörünü dikkate alarak analizler gerçekleştirip maruz kaldıkları operasyonel riski hesaplayacaklardır. Böylelikle, piyasa riski hesaplamasında olduğu gibi ya da kredi riski hesaplaması için öngörüldüğü gibi operasyonel risk için de ayrılması gereken sermaye miktarı azalacaktır[78].

Komite, bu yaklaşımın içermesi gereken niteliksel ve niceliksel kriterleri detaylandırmış, ama operasyonel riskin çok yönlülüğünden ve diğer risklerden ölçüme ilişkin metotlar açısından farklılığından ve aynı zamanda da riski ölçebilecek birçok farklı yöntemin bankalarca özgün bir şekilde geliştirilmesi amacıyla her hangi bir ölçüm metodolojisi belirtmemiştir[79]. Bu bağlamda, yeni uzlaşı bankalara söz konusu kriterleri karşılamaları koşuluyla kendi operasyonel risk ölçüm metotlarını geliştirmelerini ve hesapladıkları riske göre de yeterli olan sermaye tahsisini yapma haklarını tanımaktadır. Tabii ki böyle bir esneklik ve inisiyatif tanınmasına bağlı olarak da bankaların geliştirdikleri ve kullanacakları operasyonel risk ölçüm yöntemini ilgili yerel denetim otoritesinin onayından geçirmeleri gerekmektedir.

Komite, bankların ellerindeki veri setlerini niteliğinin ve niceliğinin denetlenmesi sürecinde ilgili yerel otoritelere yardımcı olacak belirli bazı kriterler belirlemiştir. Komite tarafından belirtilen bu kriter üç ana başlık altında ele alınmaktadır[80].

(1) Genel standartlar; banka yönetiminin süreç içerisindeki rolüne, risk yönetim sisteminin geneline ve gerekli kaynakların tahsisine ilişkin kriterlerden oluşmaktadır. (2)Niteliksel standartlar; operasyonel risk fonksiyonuna, bu fonksiyonun operasyonel

[77] Bankacılar, Operasyonel Risk Çalışma Grubu, "Operasyonel Risk İleri Ölçüm Yaklaşımları Kullanılarak Ekonomik Sermaye Hesaplaması, İleri Ölçüm Yaklaşımları-Ekonomik Sermaye İlişkisi",TBB, 2006, Sayı.58,s.97.
[78] Akkizidis ve Boucherau, s.133-134.
[79] Mazıbaş, "Operasyonel Riske Bazel Yaklaşımı: Üç Yapısal Blok Çerçevesinde Bir Değerlendirme", s.7.
[80] BCBS, International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version, 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008), s.142-149.

birimlerle ilişkilerine, raporlamaya, sistemin yazılı prosedürlere dayanmasına, süreçlerin iç denetim sistemince kontrolüne ve ölçüm sisteminin denetim otoritesince ve/veya bağımsız denetim kuruluşlarınca onaylanmasına ilişkin kriterlerden oluşmaktadır. (3) Niceliksel standartlar ise; kullanılan ölçüm yönteminin güvenilirliğine, risk ölçütlerinin sermayenin hesaplanmasında kullanılabilmesi için taşıması gerekli detaylı özelliklere, kullanılan içsel ve dışsal verilere, senaryo analizlerine, is. çevresi ve iç kontrol faktörlerine ve risk azatlımı tekniklerinin kullanımına ilişkin detaylı kriterlerden meydana gelmektedir.

Diğer taraftan, bankaların ileri ölçüm yaklaşımını kullanabilmeleri için en temelde dahili kayıp vakalarının yer aldığı bir operasyonel risk veri tabanına ihtiyaçları vardır. Bu tür bir veri tabanının varlığı, dahili zarar olaylarının izlenmesi, kurumun maruz kaldığı operasyonel risklerin en iyi şekilde olaylar bazlı olarak analiz edilmesi ve bankanın risk tahminlerinin yaşanmış olayları ve etkilerini baz alarak oluşturmasını sağlayacaktır. Komite bankaların böyle bir veri tabanını şu kaynaklardan temin edebileceğini ifade etmektedir[81]: içsel veriler, dışsal veriler, senaryo analizleri ve iş ortamı ve iş kontrol sistemlerine ilişkin veriler. Böyle, böyle bir veri tabanının inşasında, kurum dışında temin edilecek olan veriler haricinde kurum içinden temin edilebilecek olanlar iç denetim birimlerinin üretmiş olduğu raporlar, bağımsız denetim şirketleri tarafından gerçekleştirilen denetimler sonucu tespit edilen bulgular, bankanın kendi iş kollarınca tutulan ve tespit edilen muhasebeye, bilgi sistemlerine, sigortaya vb. alanlara dönük kayıtlardır[82]. Elde edilen veri kayıtlarının hiç birisi tek başına yeterli olmayabileceği için çapraz kontrollerin yapılması ve birden fazla veri kaynağının bir arada kullanılması önemlidir.

Uzlaşıya göre böyle bir veritabanı en az 5 yıllık (geçiş dönemi için 3 yıllık süre uygun görülmektedir) bir süreyi kapsayan zarar verilerine sahip olmalıdır ki birçok banka için böyle istatistiksel hesaplamalara esas teşkil edecek ve belirlenen nitel ve nicel özellikleri içeren bir zarar veri setinin olmaması gelişmiş yaklaşımı kullanabilmelerinin önündeki önemli bir engeldir. Bankalarca oluşturulacak olan bu veri setine dahil olacak kayıplara ilişkin alt sınırları belirleme konusu bankaların inisiyatifinde olsa da belirlenen sınırın altında kalan zarar tutarlarının da risk tahminleri üzerinde önemli bir etkiye sahip olmayacak olması gereklidir. Bu bağlamda, bankalar özellikle etkisi yüksek ama olabilirliği

[81] BCBS, International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version, 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008), s.145-147.
[82] Teker, s.52.

çok düşük vakalara ilişkin olarak yeterli miktarda içsel verileri olmayabileceğinden hareketle dışsal kayıp verilerini de kullanabileceklerdir.

1.4.6. Ulusal Düzenlemeler

Uluslararası alanda finansal istikrarı sağlamaya yönelik olarak kurulmuş olan BIS bünyesinde faaliyet gösteren ve gelişmiş ülkelerin merkez bankaları ve banka denetim otoriteleri yetkililerinden oluşan Basel Komitesi tarafından yayımlanan tavsiye niteliğindeki kararlar ve metinler Avrupa Parlamentosu ve Konseyi Direktifleri ile Avrupa Birliği (AB) müktesebatına dahil edilmekte ve bunlara yönelik hazırlık çalışmaları AB-Türkiye müzakerelerine konu edilmektedir. Süreç içinde söz konusu kapsamdaki çalışmaların AB müktesebatına dahil edilmesi ile de BDDK uygulamalarının AB müktesebatı esas alınarak yürütülmesi zorunluluğu ortaya çıkmıştır. Bu çerçevede, Avrupa Parlamentosu ve Konseyi Direktifleri ile Basel Komitesi'nin çalışmaları, BDDK ve dolayısıyla da bankacılık sektörü için büyük önem arz etmektedir. AB Direktiflerini birincil, Basel Komitesi'nin çalışmalarını ikincil referans olarak dikkate alan BDDK; sermaye yeterliliği, risk yönetimi, bilgi sistemleri güvenliği gibi konularda operasyonel risk yönetimine ilişkin düzenlemeleri bankacılık mevzuatımıza kazandırmaktadır. BDDK'nın bu alanda yaptığı temel düzenlemelere bu bölümde aşağıda yer verilmektedir.

Bankacılık sektörümüzün Basel-II'ye 01.01.2009 tarihinde geçişine yönelik BDDK tarafından yürütülen çalışmalar sonucunda önemli mesafeler kaydedilmiş olmakla beraber, 2008 yılının son çeyreğinde başlayan uluslararası finansal piyasalarda yaşanan sebepleri ve etkileri derin ve belirsiz gelişmeler ışığında özellikle seküritizasyon ve likidite riski açılarından Basel-II uzlaşısında eksiklikler tespit edilmiştir. Söz konusu eksikliklerin giderilmesi amacıyla ilgili dokümanlarda değişiklik çalışmalarının uluslararası düzeyde devam ettiği bilinmektedir. Bahsi geçen değişiklik çalışmaları yanında, uygulama sonuçları bu süreçte oldukça önemli olan Türk Ticaret Kanunu tasarısının henüz yasalaşmaması, finans ve reel sektör temsilcilerinin Basel-II'nin uygulanma zamanlamasına ilişkin görüşleri de dikkate alınarak bankaların sermaye yeterliliğinin ölçümünde esas alınacak kredi riskinin derecelendirmeye dayalı olarak hesaplanmasına ilişkin uygulamanın ileri bir tarihe ertelenmesinin uygun görüldüğü BDDK tarafından yapılan 25/06/2008 tarih ve 2008/15 sayılı basın açıklaması ile kamuoyuna duyurulmuştur.

1.4.6.1. Bankaların İç Sistemleri Hakkındaki Düzenlemeler

BDDK tarafından 08/02/2001 tarihli ve 24312 sayılı Resmi Gazete'de yayımlanan "Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmelik" Bankacılık sistemimizde gerçekleştirilecek olan iç denetim ve risk yönetimi ile ilgili genel çerçeveyi belirleyen ilk Yönetmeliktir. Bu Yönetmelik 01/11/2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan "Bankaların İç Sistemleri Hakkındaki Yönetmelik" ile yürürlükten kalkmıştır.

Dört kısımdan oluşan yeni Yönetmeliğin temel amacı, bankaların kuracakları iç kontrol, iç denetim ve risk yönetim sistemlerine ve bunların işleyişine ilişkin usul ve esasları düzenlemektir.

Birinci kısımda bankalarda kurulacak iç sistemlerle ilgili olarak Yönetim Kurulunun, Denetim Komitesinin ve Üst Düzey Yönetimin görev, yetki ve sorumluluklarından bahsedilmektedir. İkinci kısımda banka içinde bankanın varlıklarının korunmasını, faaliyetlerin etkin ve verimli bir şekilde Kanuna ve ilgili diğer mevzuata, banka içi politika ve kurallara ve bankacılık teamüllerine uygun olarak yürütülmesini, muhasebe ve finansal raporlama sisteminin güvenilirliğini, bütünlüğünü ve bilgilerin zamanında elde edilebilirliğini sağlamak amacıyla tesis edilmesi gereken iç kontrol sisteminden bahsedilmektedir. Yönetmeliğin üçüncü kısmında iç denetim faaliyetleri ve çalışma esasları anlatılmakta ve yapılacak denetimlerin riske dayalı, risk bazlı olması kavramı üzerinde durulmaktadır. Yönetmeliğin son kısmında risk yönetim sisteminin amacı kapsamı, risk yönetim politikaları ve uygulama usulleri, limitler anlatılmakta, risk yönetimi personelinin görev, yetki ve sorumlulukları açıklanıp, risk ölçüm yöntemleri, senaryo analizi ve stres testleri hakkında bilgi verilmektedir.

1.4.6.2. Sermaye Yeterliliği Düzenlemeleri

Basel Bankacılık Komitesi 1988 yılında riske dayalı ilk sermaye yeterlilik uzlaşısını açıklamıştır. Bu düzenlemenin ülkemize yansıması 26 Ekim 1989 tarihinde yayımlanan 3182 sayılı Bankalar Kanunu'na ilişkin 6 no.lu Tebliğle olmuştur. Tebliğde *Sermaye Tabanı/Risk ağırlıklı Varlıklar ve Gayrinakdi Krediler ve Yükümlülükler* oranı asgari %5 ile uygulanmaya başlanmış ve her yıl bir puan artırılarak 1992 yılında %8'e ulaşmıştır.

Sermaye yeterliliği standart oranında zaman içinde muhtelif değişiklikler yapılmıştır. En kapsamlı değişiklik BDDK tarafından 10/02/2001 tarihinde yayımlanan "Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik" ile yapılmış ve düzenlemeye piyasa riski bileşeni ilave edilmiştir.

Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin 01/11/2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan en son yönetmeliğin temel amacı bankaların maruz kalınan riskler nedeniyle oluşabilecek zararlara karsı konsolide ve konsolide olmayan bazda yeterli özkaynak bulundurmalarının sağlanmasına ilişkin usul ve esasları düzenlemektir. Yönetmelikte kredi ve piyasa riskine esas tutarın hesaplanması, bahse konu riskler için sermaye yükümlülüğünün standart metoda göre hesaplanması, operasyonel riske esas tutarın temel gösterge, standart yöntem ve alternatif yönteme göre hesaplanma kriterleri açıklanmakta, sermaye yeterliliği standart oranının asgari %8 olarak idame ettirilmesinin şart olduğu belirtilmekte ve BDDK'ya yapılacak bildirimlere ilişkin esaslar anlatılmaktadır.

Yönetmelikte minimum sermaye gerekliliği, sermayenin risk ağırlıklı aktiflere oranı şeklinde hesaplanmakta ve en az %8 olması istenmektedir. Risk ağırlıklı aktiflerin toplamı piyasa ve operasyonel risk için hesaplanan tutarların 12.5(%8'in tersi) ile çarpıldıktan sonra kredi riski için hesaplanan tutara eklenerek bulunmaktadır. Uygulamaya geçilmeden önce Komite bu sistemin kalibresini belirleyecektir. Sermaye gereksiniminin hesaplanması için bir çarpan katsayısı kullanabileceği gibi, riske daha fazla duyarlı daha gelişmiş metotların kullanılmasını da teşvik edebilecektir[83].

Sermaye yeterliliği oranı hakkındaki düzenlemeler 2005 yılına kadar Tebliğ ve Yönetmeliklerle yapılırken, konu 5411 sayılı Bankacılık Kanunu'nun 45'nci maddesinde münhasıran yer bulmuştur.

1.4.6.3. Bilgi Sistemleri ile İlgili Düzenlemeler

Bilgi teknolojilerinden (BT) kaynaklanan riskler, özellikle operasyonel riske neden olan, sistem kaynaklı riskler grubunda tartışılmaktadır. BT kaynaklı riskler sadece

[83] Eken, s.3-4.

operasyonel riskin sistem kaynaklı tarafını değil insan, süreç ve dışsal faktör kaynaklı bölümlerini de kısmen kapsamaktadır. Bilgi sistemlerinin önemi özellikle ülkemizde yaşanan İmar Bankası olayından sonra iyice artmıştır.

Basel Komitesi de operasyonel riskler içerisinde yer alan bilgi sistem kaynaklı risklere, özellikle Basel-II uzlaşısında yer vermiş ve sermaye yeterliliği gereksinimine operasyonel riski de dahil etmiş ve BDDK'da konunun artan önemine binaen yaptığı düzenlemelerde bilgi sistemlerine yer vermiştir. BDDK'nın bilgi sistemleri denetimi için esas aldığı ilkeler iç denetim, bağımsız denetim ve otorite denetimi olarak üç saç ayağına oturmaktadır.

Bilgi sistemleri denetiminin ***"iç denetim"*** ayağında Kurul'un yürürlükteki şu iki düzenlemesi göze çarpmaktadır:

- 01/11/2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Bankaların İç Sistemleri Hakkındaki Yönetmelik"

- 14/09/2007 tarih ve 26643 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ".

Bankaların İç Sistemleri Hakkındaki Yönetmeliğin "Bilgi Sistemlerinin Tesisi" başlıklı 11'nci maddesinde

- Bilgi sistemlerinin güvenilirliğinin sağlanması ve düzenli olarak güncellenerek gerekli değişikliklerin yapılması zorunluluğu,

- Bankalar faaliyetlerinin, bilgi sistemlerinde kesilmeler yaşandığı durumlarda dahi kesintisiz devam etmesinin sağlanmasına yönelik olarak, bilgi sistemlerinin bir tehlikeye maruz kalmadan kurtarılması ve benzeri konularda destek hizmeti alınması imkanlarını da dikkate almak suretiyle, faaliyetleri yeniden başlatma ve devamlılık sağlama planları oluşturmak ve bunları dönemsel olarak test etmek zorunluluğu,

- Bankaların bilgi sistemlerinin unsurları ile kontrolüne ilişkin asgari usul ve esasları belirlemeye Kurul'un yetkili olduğu.

İfade edilmektedir.

14/09/2007 tarih ve 26643 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ"de yer alan temel başlıklar aşağıda sıralanmıştır.[84] Tebliğ'in "Geçiş Süreci"'ne geçici maddesinde bankaların mevcut faaliyet ve sistemlerini, 2010 tarihine kadar Tebliğ hükümlerine uygun hale getirmeleri hükmü yer almaktadır. Bu Tebliğ hükümleri bankaları bir bakıma, uluslararası kabul görmüş bilgi teknolojileri kontrol hedefleri sunan COBIT dokümanlarında yer alan usul ve esaslar ile uyumlu hale getirmeyi amaçlamaktadır.

- Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi (Madde 7)
- Kimlik doğrulama (Madde 9)
- İnkar edilemezlik ve sorumluluk atama (Madde 10)
- Görevler ayrılığı prensibi (Madde 11)
- Yetkilendirme (Madde 12)
- İşlemlerin, kayıtların ve verilerin bütünlüğü (Madde 13)
- Denetim izlerinin oluşturulması (Madde 14)
- Veri gizliliği (Madde 15)
- Müşteri bilgilerinin mahremiyeti (Madde 17)
- Bilgi sistemlerine ilişkin iş sürekliliği ve kurtarma planı (Madde 18)
- Acil ve beklenmedik durum planı (Madde 19)
- İnternet Bankacılığı için benzer hükümler (Madde 26, 27, 28, 29 ve 31)
- ATM güvenliğine yönelik düzenlemeler (Madde 32)
- Kablosuz haberleşme teknolojileri (Madde 33)

Bilgi sistemleri denetiminin ***"bağımsız denetim"*** ayağında Kurul'un yürürlükteki şu düzenlemeleri göze çarpmaktadır:

[84] İlkeler Tebliği'nde yer alan başlıkların bazı kısımları BIS'ın Temmuz 2003 tarihli "Risk Management Principles for Electronic Banking" dokümanı ile ISACA'nın COBIT 4.01 dokümanında bulunmaktadır.

- 16/05/2006 tarih ve 26170 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik

- 05/12/2006 tarih ve 26367 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğ

Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik 5411 sayılı Bankacılık Kanununun 15 inci maddesi ve 93 üncü maddesinin dördüncü fıkrası hükümlerine dayanılarak bankaların bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesiyle ilgili usul ve esasları düzenlemek amacıyla hazırlanmıştır. Yönetmelikte bu denetimi yapmak için yetkilendirilecek kuruluşlarda aranan şartlar, tarafların yükümlülükleri, yapılacak bilgi sistemleri denetiminin kapsamı, türü, COBIT kapsamında denetlenecek noktalar, uygulama kontrollerinin denetimi ve denetim raporunun hazırlanmasına ilişkin hükümler yer almaktadır.

Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğ, yukarıda bahsi geçen Yönetmelik kapsamında hazırlanacak olan denetim raporunun içerik ve şekline ilişkin usul ve esasları düzenlemektedir.

Bilgi sistemleri denetiminin ***"otorite denetimi"*** ayağını ise Kurul'un bizzat gidip yerinde denetim yapması oluşturmaktadır. Risk odaklı denetim yaklaşımı ile BDDK bankalarda bilgi sistemleri denetimi yapmayı planlamaktadır.[85]

1.5. Operasyonel Risk Yönetiminin Unsurları ve Araçları

Bu kısımda operasyonel risk yönetiminin alt unsurlarını oluşturan; risk toleransı, operasyonel risk yönetiminin aktörleri, risk haritalarının ve anahtar göstergelerin

[85] Rıfat Deregözü, **"Bankacılıkta Bilgi Sistemleri Denetim- BDDK Yaklaşımı ve Bilgi Güvenliği",** Tübitak UEKAE Bilgi Teknolojileri Güvenliği Konferansı, İstanbul: Harbiye Askeri Müzesi, 13-14 Mart 2008.

belirlenmesi ve operasyonel risk kayıp veri tabanının hazırlanması konularında bilgi verilecektir.

1.5.1. Risk Toleransı

Risk toleransı, kurumun hedeflerine ve stratejik amaçlarına ulaşması amacıyla üstlenebileceği risk düzeyine ilişkin referansları ifade eden, yönetimin risk yönetimi anlayışının yansımasıdır[86]. Riski kabul etmenin ve üstlenmenin maliyetiyle riski üstlenmemenin maliyeti karşılaştırılarak makul bir dengenin (kabul edilebilir risk seviyesi) belirlenmesi gerekir. Risk toleransının statik ve durağan olmayıp[87] yönetim tarafından değişen koşullara ve kurumun maruz kaldığı risklere karşı esnetilebilir veya sıkılaştırılabilir.

Risk toleransı, risklerin değerlendirilmesi, gözlenmesi ve kontrolüne ilişkin alanlarda önemli bir rol oynar ve personele risklerin önem ve etki derecelerine göre, riskleri gözlemleme ve kontrol etmeye dönük faaliyetlerinde önceliklendirme yapmalarında yardımcı olur[88].

Kurumsal risk toleransının tanımlanması ve uygulanması şu şekilde gerçekleşmektedir: Yönetim kurulu ve üst yönetim, kurumun hedeflerinin bir parçası olarak kurumun üstlenebileceği risk miktarı ve kapasitesi doğrultusunda risk toleransını belirler. Birim yöneticileri ve çalışanlar ise belirlenmiş olan limitler ve sınırlar dahilinde birim seviyesinde altı limit ve sınırları belirler. Birimler ve işlemler düzeyinde tanımlanmış olan limitler, göstergeler, esnek sınırlar gözlemleme ve raporlama yapabilmek için bilgi sistemine entegre edilir. İç denetçiler ise, birimlerin faaliyetlerinin kurumsal risk toleransı tanımı doğrultusunda ne ölçüde yerine getirildiğini denetler ve üst yönetime raporlama yapar.(4)

Etkin bir risk yönetimi süreci ve risk toleransının en verimli şekilde kurum içinde delege edilmesi belirli bir hiyerarşik yapıyı gerektirir. Belirli düzeylere yaklaşan ve onları aşan risklerin bir üstteki karar vericiye geçmesi için belirlenmiş olan sınırlar vardır. Böylelikle bir üstte yer alan personel veya birim de maruz kalınan riskin ne şekilde

---

[86] Frost, s.30.
[87] **"Enterprise-wide Risk Management for Insurance Industry"**, Global Study, PWC,2004'den Chapman, s.186.
[88] LLOYD'S, "Risk Management Toolkit", http://www.lloyds.com, (12 Ocak 2007), s.34.

yönetileceği konusunda karar verir. Kurumun maruz kaldığı riskler geniş bir alanı kaplıyorsa, üst yönetim bazı risk konularında daha az riske maruz kalmayı tercih edip diğer taraftan diğer bazı risk alanlarında ise daha fazla riske girmeyi değerlendirebilir. Böylelikle, kurumun genel ve ortalama olarak maruz kaldığı risk düzeyinde farklılık oluşmamış olacaktır.

Kurumsal risk toleransının ölçüsünün ne olması gerektiği konusunda net oranlar ve rakamlar vermek kolay değildir. Bazı kurumlar riske bakışlarını "muhafazakar" ya da "agresif" olarak nitel bir şekilde tanımlarken bazı işletmeler, risk toleransını yüksek, orta düzey ve düşük düzey gibi kalitatif yöntemlerle, diğer bazı işletmeler ise gelir, risk ve büyüme hedefleri üzerinden hareketle kantitatif yöntemlerle değerlendirmektedir[89]. Kurumsal risk toleransını ifade eden parçalar nitel ve nicel ifadeler içerebilir. Risk toleransının nitel ifadelerle belirlenmesi, özellikle sayısallaştırmanın zor olduğu alanlarda kullanım ve anlaşılması açısından kolaydır, ancak karlaştırma yapmaya uygun olmadığı gibi maruz kalınan riskler arasında bir sıralama yaparken de öznellik ön plana çıkmaktadır. Risk toleransı yüksek olan bir şirket, sermayesinin önemli bir bölümünü yeni iş alanlarına girmek gibi riski yüksek alanlara yatırabilir. Buna karşın, risk toleransı daha muhafazakar olan bir şirket ise, sadece önemli seviyede tecrübesi olduğu ve doyum seviyesinde olan sektörlere yatırım yaparak kayıp riskini azaltmayı tercih edebilir. Dolayısıyla, risk toleransı kurumun stratejisi ile doğrudan ilişkilidir ve kurum maruz kaldığı değişik riskler karşısında stratejisini oluştururken dikkate alır.

Risk toleransı kendi içinde kurumsal, delege edilmiş ve proje kaynaklı risk toleransı olarak 3 farklı türde oluşturulabilir[90]. Kurumsal risk toleransı olarak, yönetim kurulu tarafından belirlenen ve kurumun maruz kalabileceği azami risk miktarı tarif edilmektedir. Bu risk toleransı tek bir tutar olmayabilir ve personel, sistem, süreçler, dışsal riskler vb. şeklinde alt limitlere göre düzenlenebilir. Yönetim kurulu ve üst yönetim, kurumun üstlenebileceği maksimal risk düzeyi ile kurumun kabul edilemez olarak gördüğü risk seviyelerini belirler. Delege edilmiş risk toleransı ile anlatılmak istenen ise, kurumsal

---

[89] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **Enterprise Risk Management Integrated Framework, Executive Summary Framework,** New York, AICPA, September 2004, s.19-20.

[90] **The Orange Book**, Management of Risk-Principles and Concepts,2004, HM Treasury, http://alberta.ca/home/documents/orange_book_mgmt_risk.pdf, (10 Ağustos 2006), s.24.

risk toleransının üst yönetimden daha aşağıda yer alan birimlere doğru ve her bir birimin ne oranda ve ne seviyede risk üstlenebileceğini düzenleyen bir tanımlamadır. Bu çerçevede, daha alt birimlerde yüksek düzey olarak nitelenen bir risk toplamı daha yukarıda yer alan üst yönetim değerlendirmesinde çok daha geniş bir bakış açısından hareketle yeterince riskli olmadığı şeklinde değerlendirilebilir. Proje kaynaklı risk toleransı ise, kurumun günlük operasyonlarından bağımsız olarak kurumun geliştirmekte olduğu bir projeden kaynaklanabilecek olan maksimal risk düzeyini tanımlar. Farklı projeler, doğal olarak farklı düzeyde risk toleransı barındırır ve risk toleransını geniş tanımlamış olan bir kurum önemli düzeyde gelir elde etme olanağına sahip oluyor.

1.5.2. Operasyonel Risk Yönetiminin Aktörleri

Kurumun yönetiminde ve denetiminde rol aldıkları için risk yönetim sürecinin etkin bir şekilde işlemesiyle ilgili olarak bir çok sorumlu bulunmaktadır. Yönetim kurulu, üst yönetim, iç denetçiler kurum içi önemli aktörleri oluştururken, bağımsız dış denetçiler ve resmi denetim elemanları da kurum dışı önemli aktörleri oluştururlar[91].

Yönetim kurulu ve üst yönetim, kurumsal operasyonel risk yönetiminin etkin çalışmasından en üst düzeyde sorumludur. Diğer taraftan, operasyonel risk çerçevesinin, bütüncül olarak kurum çapında değerlendirilebilmesi için kurum bünyesinde bağımsız bir operasyonel risk yönetimi bulunmalıdır. Söz konusu birimin görev ve sorumlulukları net olarak belirlenmeli ve yazılı hale getirilerek tüm süreçlerde, prosedürlerde ve uygulamalarda tutarlı ve benzer yaklaşımların gerçekleştirilmesi sağlanmalıdır. Bu birim, büyüklük, görev ve yetki seviyesi açısından kurumun operasyonel risk büyüklüğü ile orantılı olmalı, ancak operasyonel birimlerden bağımsız olmalıdır. Bu birim, operasyonel risk yönetim süreci bağlamında gerekli olan politika, prosedür ve süreçlerin geliştirilmesini sağlamalı, operasyonel riskin kurumca kabul edilen tanımını yapmalı, operasyonel riskin yönetilmesine ilişkin gerekli olan yöntem ve araçlar üzerinde çalışmalarda bulunmalı, birimler arası koordinasyonu sağlamalı, analizler yaparak belirli normları belirlemelidir[92].

İç denetçilerin, operasyonel riskin ölçülmesi, değerlendirilmesi ve raporlanmasına ilişkin süreçlerin etkin çalışıp çalışmadığına dönük yönetime belirli bir güvence sağlamak,

[91] Akkizidis ve Bouchereau, s.80-85.
[92] Moosa, s.202.

kurum çapında en fazla risk unsuru taşıyan alanları ve faaliyetleri belirlemek, risk haritaları oluşturmak, riskler ve kontroller arasındaki uyumu ve etkinliği değerlendirmektir. İç denetçiler, riskler ve kontrol noktaları arasındaki bağlantıları ve bu bağlantıların etkinliğini değerlendirmek için gerekli olan teknik ve yöntemleri geliştirerek kurumsal seviyede risk yönetiminin temel ilkelerinin daha iyi anlaşılmasını sağlayacaktır.

Birim yöneticilerinin, kendi sorumluluk alanlarına ilişkin operasyonel riskleri en iyi şekilde yönetmeleri beklenir. Kendi birimleri çapındaki operasyonel risk yönetiminden sorumludurlar ve kendi birimlerindeki ORY uygulamalarının kurumsal düzeyde belirlenmiş olan ilkelerle uyumlu olmasını sağlamalıdırlar. Birim yöneticileri, bir taraftan operasyonel riskleri getiri, fırsat dengesinden hareketle yönetirken diğer taraftan da operasyon kaynaklı risklerini yönetmelidirler.

Kurumun, mali işlerden sorumlu üst yetkilisi ve insan kaynaklarından sorumlu üst yetkilisi de operasyonel risklerin en etkin şekilde yönetilmesini teminen gerekli olan kaynağı ve personeli sağlamalıdır. Burada bahsettiğimiz, üst düzey yöneticilerin operasyonel risk yönetimi kapsamındaki sorumluluklarının yanı sıra kurumda çalışan en alt düzeydeki personel bile karşılaştığı riskleri değerlendirmeli, kendi görev alanlarında risk azaltıcı yöntemleri kurumsal ilkeler doğrultusunda uygulamalıdır. Bağımsız dış denetçiler ve düzenleyici kurumların denetçileri de kurumun operasyonel risk yönetiminin etkinliğini değerlendirmek ve gerekli önerileri ve kritiklerini belirtmek durumundadırlar. Diğer taraftan kurum ile beraber çalışan sigorta şirketleri ya da güvenlik şirketleri de kurumun operasyonel risk yönünden bir değerlendirmesini yapmaktadırlar.

1.5.3. Risk Değerlendirme Araçları

Risk değerlendirme araçları başlığı altında; özdeğerlendirme, risk haritaları ve anahtar göstergeler sayılabilir. Aşağıda bu kavramlar hakkında gerekli açıklamalara yer verilmiştir.

1.5.3.1. Öz Değerlendirme Teknikleri (Self Assesment)

Öz değerlendirme yönteminde, personelden kendi dahil olduğu iş süreçlerinin içerdiği risklere ilişkin kontrollerin güçlü ve zayıf yönlerini değerlendirilmesi ve böylece tahminlerden hareketle maruz kalınan risklerin ölçülmesi amaçlanmıştır.

Özellikle geçmişe dönük veri tabanı eksikliğinin önemli boyuta olduğu ortamlarda bu tür bir risk değerlendirme tekniği işe yaracaktır[93]. İş birimleri, kendi birimlerini ilgilendiren faaliyetlerine ilişkin olarak maruz kaldığı risklerin şiddeti, sıklığı ve en kötü durumda yol açacağı zarara ilişkin tahminleri oluştururlar.

Öz değerlendirme sürecinde birden fazla yöntem ve araç kullanılabilmektedir. Kurumların faaliyet sınırları değiştikçe, risklilik değerlendirmeleri de değişecek olup kullandığı yöntemlerde de çeşitli revizyonların olması muhtemeldir. Öz değerlendirme araçları içinde öncelikle kullanılan çalışanlar tarafından doldurulan çeşitli anketsel soru setleridir. Diğer kullanılan bir araç da, çalışanların kendi görüş ve önerilerini belirttiği grup çalışmalarıdır. Bu tür görüşmelerde, ilgili birimde çalışan personelin karşılaştığı riskler, bu risklere ilişkin geliştirilmiş olan veya geliştirilmesi gereken kontrol noktaları ve yapılması gerekenler tartışılır. Bu tür risk değerlendirmelerinin belirli periyotlarda yapılması ve üretilen raporların ve çalışma sonuçlarının da üst yönetimin çalışma yöntemiyle ve bilgi ihtiyaçlarıyla uyumlu olması önemlidir[94].

Her ne kadar öz değerlendirme bir risk ölçme yöntemi olsa da kendisi de bir risk unsuru oluşturmaktadır. Bu yöntemin gerçekleştirilmesi sürecinde katılıcıların vermiş olduğu yanıtlar, değerlendirmeler onların objektif görüşlerini yansıtmıyor olabilir. Bu yüzden yöntem bir “moral hazard” problemi ile yüz yüzedir, çünkü operasyonel risk ancak birimden bir çalışanın riskle ilgili bahsetmesiyle gün yüzüne çıkar veya risk olarak değerlendirilmesini istemediği noktaları ise bilerek atlayabilir[95]. Bu tür riskleri azaltmak amacıyla, risk uzmanların sürece katılımı sağlanabilir, birimler tarafından yapılacak olan

[93] Marcelo G.Cruz, **Operational Risk Modeling Theory and Practice**, Navara:Risk Books, 2004, s.119.
[94] Frost, s.235-237.
[95] Cruz, s.119.

değerlendirmeler ile tutarlılık sağlanabilir, veya iç kontrol de sürece dahil edilerek bu yöntemin nitel unsurları azaltılabilir.[96]

Öz değerlendirme her ne kadar sofistike bir yöntem olmasa da, kurumun yüz yüze olduğu operasyon kaynaklı risklerin yönetilmesinde yönetime belirli bir hareket rehberlik alanı sağlar. Üstelik, bu yöntem oldukça düşük maliyetli ve gerçekleştirmesi de basit olup üst yönetimin kararlar alırken risklere ilişkin nitel değerlendirmelere bilmesi de oldukça önemlidir[97].

1.5.3.2. Risk Haritaları

Risk haritası bir kurumun, tüm süreçlerini, birimlerini ve görev ve sorumlulukları detaylandıran ve önemli risk noktalarını gösteren bir özettir. Her bir birim yöneticisine ve personele kadar görev ve sorumlulukları bağlamında maruz kalabilecekleri riskleri belirlediği için kapsamlı bir araçtır. Risk haritaları, aynı zamanda süreçlerdeki zayıf noktaları tespit ederek risk yönetimine ilişkin alt yapı sağlar. Ama, öz değerlendirme yöntemi gibi kullanılan ve elde edilen veriler nitel ve göreceli olduğu için üst yönetimin karar verme sürecinde yüksek düzeyde bir güven sağlamayabilir.

1.5.3.3. Anahtar Göstergeler

Operasyonel risk yönetiminde anahtar göstergeler öncü göstergeler olarak da isimlendirilebilir. Bunlar anahtar performans göstergeleri ve anahtar risk göstergeleri olarak işlevlerine ve baz aldıkları veriye göre farklı türlere ayrılırlar. Belirlenmiş risk göstergeleri izlenirken, bu göstergelerdeki belirgin değişimlerin kayıp riskini arttıracağı varsayımı ile hareket edilerek; risk göstergelerinin uyarı sinyali olarak kullanılması ve uyarı halinde riske karşı önlem alınması amaçlanmaktadır. Dolayısıyla risk göstergeleri operasyonel risk yönetiminde nereye odaklanılması gerektiğini gösteren, kurum bünyesinde risk bilincinin oluşmasına katkı yapan, üst yönetim, risk yönetimi ve kurumun diğer iş birimleri arasında iletişimin kurulmasını sağlayan araçlardır.

---

[96] **Bankacılar Dergisi**, Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, "Operasyonel Risk Veri Tabanı",TBB, Haziran 2004, Sayı.48, s.135-137.

[97] Gerrit Jan van den Brink, **Operational Risk, The New Challenge for Banks,** 1.Baskı, New York:Palgrave Publishers Ltd., 2002, s.69.

Risk göstergeleri her kurumun kendi kültürüne, risk toleransına, organizasyonel yapısına, büyüklüğüne bağlı olarak kurumdan kuruma farklılık arz edebilmektedir. Yani her kuruma uygulanabilecek standart bir anahtar göstergeler listesinden bahsetmek zordur[98].

1.5.3.3.1. Anahtar Performans Göstergeleri

Anahtar performans göstergeleri (APG), kurumun faaliyetlerine, iş hacimlerine ve gerçekleşmelere göre kurumca belirlenen çeşitli ölçütleri ifade eder[99]. Yönetim, kurumun performansını yansıtan ve ilk bakışta anlayabilecekleri temel göstergelere ihtiyaç duyar; çünkü ancak bu tür göstergeler vasıtasıyla kurumun performansına ilişkin değerlendirmelerini hızlı bir şekilde yapıp gerektiğinde ve şartlar değiştiğinde de inisiyatif kullanır. Spesifik performans göstergeleri her ne kadar sektörden sektöre ve şirketten şirkete farklılık gösterse de benzerlik arz ettiği bazı temel noktalar da vardır[100]: Müşterilerin memnuniyet seviyelerini gösteren endeksler müşteri ilişkilerine; işçilik maliyetleri, çalışan başına verimlilik ve sermaye getirisi gibi göstergeler işletmenin faaliyetlerine ve karlılığına; eğitim masrafları, ortalama personel verimliliği gibi göstergeler insan kaynaklarına; zamanında teslimat, bakım masraflarına ilişkin veriler tedarikçilere; satışlar, maliyetler, brüt/net kar marjı, aktif karlığı gibi göstergeler kurumun mali performansına; ciddi kazalar, kayıplar, ödenen tazminatlar ve sigorta bilgileri gibi göstergeler de güvenlik ve çevreye ilişkin kanaat sahibi olunmasına yardımcı olarak ilgili süreçlerin performans düzeylerinin tespitinde belirleyici olur.

Yukarıda bahsedilen temel anahtar performans göstergelerine ilişkin çok farklı performans ölçütlerinden bazıları Tablo 5'de örneklendirilmiştir.

---

[98] Babuşçu, s.157-158.
[99] G. Sampson, D. Kumar ve D. Lau Andersen, "Firmwide Issues for Financial Institutions: Risk Model Selection", Sarah Jenkins(Ed.), **Advances inOperational Risk Firm-wide Issues for Financial Institutions**, Somerset:RiskBooks, 2001, s.99.
[100] Akkizidis ve Bouchereau, s.178.

Tablo 5: Anahtar Performans Göstergelerine Örnekler

PERFORMANS GÖSTERGESİ ÖLÇÜTÜ	ÖRNEK
Planlanan zaman	Dokümanın % 90'ının zamanında tamamlanması
Sürecin tamamlanma periyodu	Bir fatura üzerindeki işlemlerin ortalama 3.5 gün içerisinde tamamlanması.
Verimlilik	Her gün ortalama olarak 50 adet başvurunun işlenmesi.
Kalite	Her 100 üründen ortalama 4.2 adetinde hata çıkması.
Maliyetler	Bir dokümanın işleme alınmasının maliyetinin 10 YTL olması.
Asgari ve azami referans seviyeleri	Mevcut performansa ilişkin verilerinin izlenmesi.
Dönemsel değişimler, trendler	Zaman içerisindeki performans değişimlerinin değerlendirilmesi.
Kontrollere ilişkin ölçümler	İşler ve performansın daha önceden belirlenmiş olan aralıklarda seyredip seyretmediğine ilişkin,
Tespite yönelik ölçütler	Herhangi bir problemin sebebini ve nerede gerçekleştiğini tespite yönelik çalışma.
Planlama ölçütleri	Geçmiş ve güncel performansa bakarak geleceğe ilişkin öngörülerin geliştirilmesi.

Kaynak: Şenol Babuşçu, **Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi**, Ankara: Akademi Consulting&Training, Eylül 2005, s.158.

APG'ni tanımlarken, bunların kurumun genel faaliyetlerine ilişkin mi yoksa kurum içerisindeki bir birimin gerçekleştirmesi gereken bir hedefe mi yönelik olduğunun net şekilde ortaya konması gerekmektedir. Çünkü amaçlanan hedefe ulaşmakta tanımlanan performans göstergelerinden yola çıkılmaktadır. Dolayısıyla bu göstergeler bir kurumun veya kurum içerisindeki her bir birimin hedeflerini değerlendirmede kullandığı, ölçüm ve değerlendirme yaptıkları süreç ve operasyonlarla hedefler arasındaki temel bağlantıdırlar.

1.5.3.3.2. Anahtar Risk Göstergeleri

Anahtar risk göstergeleri (ARG), bir veya birden fazla başarı faktörünü gösteren kantitatif metriklerdir[101]. Bu metrikler yönetime kurumun maruz kaldığı risklere ilişkin olarak detaylı ve özellikli bilgiler sunarak üst yönetimin risk yönetimine ilişkin alacağı kararları

[101] Peter Vinella ve Jeanette Jin, "A Foundation for KPI and KRI", Ellen Davis (Ed.), **Operational Risk Practical Approaches to Implementation**, Navara:Risk Books, 2005, s.163.

şekillendirmesinde oldukça kullanışlıdırlar. Basel Komitesi anahtar risk göstergelerini şu şekilde tanımlamaktadır: *" ..bir bankanın risklilik durumunu yansıtan genellikle mali verilerden hareketle belirlenen istatistiki ve ölçülebilir rakamlar ve değerlerdir. Bu göstergeler, aylık veya çeyrek dönemler gibi belirli periyotlarda gözden geçirilerek kurumun maruz kalabileceği risklere karşı bilgilenmesini sağlar..."*[102]. ARG, kayıpların gerçekleşmesinden önce fark edilerek engellenmesinde veya etkisinin azaltılmasına yönelik çalışılmasında işlevseldir. Buradaki varsayım, belli risk göstergelerindeki değişimin kayıp riskini artıracağı ve risk göstergelerinin uyarı sinyali olarak kullanılarak riske karşı önlemlerin alınabileceğidir.

ARG, kurumun maruz kaldığı anlık riskleri ve bu riskler karşısındaki kontrol noktalarının etkinliğini göstererek kurumun risk yönetim profilini ve risk seviyesindeki değişim ve trendleri ortaya çıkarır. Kayıplara sebep olabilecek risk unsurlarında, kontrollerin etkinliğinde ve risk ortamında meydana gelen değişimleri yansıtarak gerçek bir kaybın yaşanmasını önlemek amacıyla öncül sinyal göstergeler olarak yönetime yardımcı olur. Risk göstergelerinden gelen ham verileri değerlendirebilmek ve kurumun maruz kaldığı riskler karşısında etkin kararlar verilmesini teminen önceden tanımlanmış sınırlar ve limitlerin (escalation triggers, thresholds) belirlenmesinde önemlidirler[103]. ARG'leri tanımlamanın zorlu tarafı ise, tespit edilen risklerin rakamsal ifadelere dönüştürülme sürecidir. Risk göstergelerine ilişkin bir diğer eksiklik ise, risk göstergesi ve kayba sebep olan olay arasındaki ilişkinin net bir şekilde ilişkilendirilememesi veya aradaki ilişkinin spekülatif bir şekilde açıklanmaya çalışılmasıdır[104].

Yönetim, performansını izlediği risk türüne göre risk göstergelerini günlük, haftalık, aylık veya yıllık bazda tecrübesiyle beraber kontrol ederek bazı risklerin proaktif bir şekilde yönetilmesi gerektiğine karar verebilir ve bu doğrultuda gerekli aksiyonu alabilir.

---

[102] Carol Alexander, **Operational Risk: Regulation, Analysis and Management,** London: Prentice Hall, 2003, s.25.
[103] LLOYD'S, "Risk Management Toolkit", http://www.lloyds.com/Lloyds_Market/Tools_and_reference/Risk_Management_Toolkit_home/ (12 Mart 2007), s.114-115.
[104] Frost, s.235-237.

Yönetim, risk göstergelerini aynı zamanda değişkenler arasında ilişki olup olmadığını tespit etmekte de kullanabilir. Örneğin, bazı birimlerdeki geçici personel sayısı ile o birimde yaşanan kayıplar arasında bir ilişki olup olmadığı gibi bazı korelasyon analizlerinde risk göstergeleri oldukça yararlı olabilmektedir. Risk göstergeleri aynı zamanda, yönetime ileride daha önemli sonuçlar ve kayıplar doğurabilecek riskler ile ilgili olarak hareket alanı ve zamanı sağlayarak uyarıcı bir rol de oynamış olurlar. Risk göstergelerinin ölçülebilir olması, üst yönetime kalitatif yargılardan ve kişisel yorumlardan uzak daha objektif bilgi akışı sağlayarak, iç veriler vasıtasıyla ölçülen operasyonel risk ile ölçülebilir göstergelerden elde edilen sonuçlar arasında nedensellik ilişkisi kurulabilmesine yardımcı olur.

Bir göstergenin gerçek anlamda işe yarayabilmesi ve operasyonel faaliyetlerin risklilik durumu konusunda doğru, öncül bilgi verebilmesi için gösterge ile yaşanan kayıp arasındaki nedenselliğin sıklık ve şiddet verilerinden hareketle istatistiki yöntemlerle kanıtlanmış olması gereklidir. Bu sebeple, göstergeler somut ölçümlere dayandırılabilmeli, düzenli olarak izlenen risk göstergeleriyle yaşanan, yaşanması muhtemel olan veya önleyici aksiyonlar ile yaşanması engellenen kayıplar arasındaki ilişki doğru ölçülmelidir. Operasyonel risk yönetimi kapsamında anahtar risk göstergelerinden yararlanabilmek için ayrıca, risk göstergeleri ve kayıplar ile olası kayıplar arasındaki ilişki sık sık takip edilmeli, gereken güncellemeler risk göstergelerinde gerçekleştirilmeli; risk göstergelerinin kimler tarafından, hangi sıklıkta ve hangi yöntemler ile izleneceği, kimlerin neler yapacağı ve kime raporlanacağı, açıkça ve yazılı olarak belirlenmelidir[105].

Tablo 6, operasyonel riskleri, bu risklere sebep olan temel etmenleri ve ilgili ARG'leri içermektedir. Finansal kurumlar bu türdeki operasyonel risklerle her gün karşılaştıkları için ARG'ler her bir alana ilişkin olarak belirlenmeli ve daha da önemlisi her birinin diğerlerini nasıl etkilediği tespit edilmelidir.

[105] Candan ve Özün, s.231.

Tablo 6: Operasyonel Riskin Kaynakları ve İlgili ARG

Operasyonel Risk Kaynağı	Risk Çeşitleri	Bazı Anahtar Risk Göstergeleri
İnsan	İç kontroldeki ve kurumsal yönetişimdeki aksaklıklardan kaynaklanan mali kayıplar, hatalar, ehliyetsizlikler, kurum içi veya dışından kaynaklı yolsuzluk ve hırsızlık. ***Kurum içi Yolsuzluk:*** Bilerek bazı verileri yanlış raporlamak,bazı işlemleri hiç raporlamamak,çalışan tarafından gerçekleştirilen hırsızlıklar, içerden ve dışardan bilgi sızdırma,rüşvet gibi. ***Kurum dışı Yolsuzluk:*** Soygun, kalpazanlık, bilgisayar sistemine dönük sızma ve ele geçirme girişimleri gibi. ***İşlemler ve Operasyonlar:*** Sözleşmelerde veya belgelerdeki hatalar, gizlilik kurallarına uyulmaması, gizli müşteri bilgilerinin ifşa edilmesi, para aklama, yasal izni olmayan ürünlerin satışı, yanlış veri girişleri gibi.	✓ İşlemlerde meydana gelen hataların veya istisnai işlemlerin sıklığı ve önem derecesi ✓ Gerçekleşmemiş olan ticari işlemler ✓ Personel sirkülasyon oranı ✓ Belgelendirmeye ilişkin yapılmış hatalar ✓ Personelin eğitim ve tecrübe seviyesi ✓ İşlem adetleri ve ciro ✓ Gelirler yönündeki istikrar
Teknolojik Altyapı	Kurum içi veya dışı kaynaklı olaylardan dolayı sistemde oluşan hatalar ***Kurum içi kaynaklı:*** Programlama hataları, sistemi zorlayan veya çalışmasını engelleyen yeni programların yüklenmesi, bazı verilerin kaybolması, kullanılmakta olan sistemle uyumsuz yeni programların yüklenmesi, kurum içi telekomünikasyon sorunları, sistemin alt yapısının işin gereklerini yeterince karşılamaması gibi. ***Kurum dışı kaynaklı:*** Elektrik vb kesintileri, sistemden kaynaklan ve işi durma noktasına getiren olaylar, telekomünikasyon sorunları,verilerin kaybolması, kurum dışından kaynaklanabilecek güvenlik ihmalleri gibi.	✓ Sistemin ve bazı uygulamaların çalışamaz hale gelmelerine ilişkin istatistiki bilgiler ✓ Bakım maliyetleri ve oranları ✓ Sistem kaynaklı hata oranı ✓ Kesinti sonrasında verilerde oluşan kayıplar ✓ Sistemin kesilmesi ve tekrar çalışmaya başlaması arasındaki zaman ✓ Yedeklemeye ilişkin hata oranları
Süreçler	***Süreçlerin İşleyişi:*** Süreç yönetimi, ürün ve hizmet karmaşıklığı, yönetim hataları, güvenlik noksanları, yasal dokümanların yetersiz veya hatalı olarak hazırlanması, müşteri hesaplarına yetkisiz olarak erişim, tedarik ve teslime ilişkin hatalar, ödemelere ilişkin eksiklikler, işyeri güvenliği, çalışanların tazmin talepleri, işyeri güvenliğine ve çalışan sağlığına olması gerektiği riayet	✓ Kurum politikalarına aykırı olarak gerçekleştirilmiş sözleşmeler ✓ Tahsilata ilişkin oranlar ✓ Muhasebe kaynaklı hatalara ilişkin oranlar ✓ Düzenleyici ve denetleyici kurumlarca tespit edilen eksiklikler ✓ Ödemelere ilişkin sorunlar.

	edilmemesi, grevler, ayrımcılık yapıldığına ilişkin iddialar gibi.	
Dışsal Olaylar	***Politik belirsizlikler:*** Savaş, menkul ve gayrimenkullarda oluşabilecek zararlar, yangın, salgın hastalıklar,terör eylemleri, vandalizm, gibi. ***Doğal Felaketler:*** Deprem, sel, fırtına, volkan patlaması gibi. Çevrenin korunmasına ilişkin yasal mevzuata uygun hareket edilmemesi, tedarikçilerde meydana gelebilecek iflas vb.,nakliyata ilişkin sorunlar gibi.	✓ Fiziksel kayıplar (insan,mali,sistem olarak) ✓ Kaybolan bilgi oranı

Kaynak: Ioannis Akkizidis, ve Vivianne Bouchereau "**Guide to Optimal Operational Risk and Basel II**", New York: Auercbach Pub., 2006, s.178-179.

Bazı durumlarda, sebepler, olaylar ve sonuçlar arasında net bir ayrım olmayabilir. Çünkü bir olaya ilişkin "sebep" olarak değerlendirilen bir şey, aynı zamanda başka bir olayın "sonucu" olarak da değerlendirilebilir. Örneğin hırsızlık kavramı ele alındığında çalışanların tutumlarından kaynaklanmış bir "olay" olarak görülebilir ya da finansal kurumlar için repütasyon kaybına sebebiyet verebilecek bir "sonuç" olabilir. Dolayısıyla, risk yöneticilerinin ve analistlerin sebep, olay ve sonucun ne olduğuna ilişkin bakış açıları net olmalıdır. Bu çerçevede düşünülmesi gereken iki nokta vardır:

1. "Sebep" olarak tanımlanan kavram, en az bir ya da daha fazla risk doğuran olaya sebebiyet vermelidir. "Olay" olarak tanımlanan kavram ise asgari olarak bir sebepten kaynaklanmalı ve bir veya daha fazla sonuca sebep olmalıdır. "Sonuç" olarak tanımlanan kavramında bir yada daha fazla olaydan kaynaklanması ve yeni sebepleri meydana getirmesi gereklidir.

2. Daha önceden nasıl tanımlanmış olursa olsun, ilgili kurumun/işletmenin "sebep", "olay" ve "sonuç"a yönelik tanımlara sadık kalması gereklidir. Eğer, önceki tanımda değişiklik gerekirse söz konusu değişiklik yazılı hale getirilmeli ve operasyonel risk yönetiminin sürecine ve sistemine dahil olan herkes bu değişiklikten haberdar edilmelidir.

Finansal kurumlarda gerçekleşen operasyonel risklere ilişkin tipik olay, sebep ve sonuçlar ile bunların işe olan etkileri Tablo 7'de gösterilmektedir.

Tablo 7: Operasyonel Riskin İşe olan Etkilerine ilişkin örnekler

Sebepler	Olaylar	Sonuçlar	İşe Olan Etkileri
Yetersiz Personel Sayısı	Müşteri hizmetleri servisinin müşterilerden her gün gelen çağrıların tamamını cevaplayamamaktadır	✓ Müşteriler hizmet alabilmek için daha fazla beklemek durumundalar ✓ Müşteri memnuniyeti azalacak ✓ İtibar kaybı olacak ✓ Daha az sayıda müşteri edinimi	Geleceğe dönük daha düşük bir büyüme ve ciro artışı
Teknolojik Altyapının Değişikliklerle Güncelleştirilmesi ve Geliştirilmesi	CRM tedarikçisi firma mevcut sistemi geri almayı ya da verdiği servis desteğini azaltmayı planlıyor	✓ Mevcut CRM sisteminin işleyişi ile ilgili olarak daha az servis desteği alacağız ✓ Satışları artırmak için gerekli iyileştirmeleri yapamayacağız ✓ Satış gücünde oluşacak zayıflama	Daha düşük satış oranları
Yeni Yasal Düzenlemeler	İnternet tabanlı bankacılık işlemlerine ilişkin kayıtlar 10 yıllık süreyi kapsayacak şekilde arşivlenecek Mevcut bilgi sistemleri altyapısı bu tür uygulama değişikliği için elverişli değil	✓ Yedekleme ve arşivleme sistemi yeterli değil ✓ Faaliyetlere ilişkin yaptırımlarla karşılaşabiliriz	Kurumun piyasadaki durumu ve imajıyla ilgili olarak olumsuz etkiler

Kaynak: Ioannis Akkizidis, ve Vivianne Bouchereau "**Guide to Optimal Operational Risk and Basel II**", New York: Auercbach Pub., 2006, s.181.

1.5.3.4. Operasyonel Risk Kayıp Veri Tabanı ve Karşılaşılabilecek Sorunlar

Bankaların operasyonel risk kayıp veritabanı oluşturmaları; kurumsal seviyede risk yönetimi konusunda farkındalık yaratmak, ampirik analiz ve çalışmalarda yararlanılmak, ve operasyonel risk için ayrılması gereken sermayenin hesaplanmasında kullanılmak için önemli ve faydalıdır[106].

Operasyonel riskin ölçülmesi maruz kalınabilecek risklerin etki ve olasılık düzeylerinin bilinmesi ile alakalı olduğundan gerek veri eksikliği gerekse de veri yetersizliği nedeniyle operasyonel risklerin piyasa ve kredi riskleri gibi sayısallaştırılarak ölçülmesi kolay olmamaktadır.

[106] Micheal Haubenstock, "The Operational Risk Management Framework", Carol Alexander (Ed.), **Operational Risk Regularion, Analysis and management**, London:Prentice Hall, 2003, s.251

Operasyonel risklerin özellikle ileri ölçüm yaklaşımları ile ölçülmesinde, kurumda risk kültürünün ve risk yönetim sisteminin oluşturulmasında, ölçüme yönelik sağlıklı verilerin sağlanmasında, operasyonel risk veri tabanı vazgeçilmez bir unsurdur. Bunun en önemli nedenlerinden biri, operasyonel risk verilerinin, kurumun kendi yapısına ilişkin özellikleri ve operasyonel risk profilini yansıtan en objektif ve duyarlı risk göstergeleri olmasıdır.

Kurumlar, kendi ürün ve hizmet yapısı, büyüklükleri, süreçleri, operasyonel risk ve kayıp tanımlarına uygun olarak, belirledikleri sınır dahilindeki bilgileri kaydederek kendi iç veri tabanlarını oluşturmalıdırlar.

Operasyonel risk veri tabanına ilişkin verilerin; doğruluk, tamlık, zamanında erişilebilirlik, tutarlılık gibi nitelikleri taşıması, kolay, anlaşılabilir ve risk yönetim sürecinde rahatlıkla kullanılabilir olması, kurumun risk yönetim yaklaşımına uygun olması sağlanmalıdır[107].

Operasyonel risk veri tabanına girdi sağlayan ve tüm bankalarda bulunan temel veri kaynakları; iç denetim, iç kontrol ve dış denetim raporları, muhasebe, hukuk, bilgi işlem, güvenlik ve sigorta kayıtları ile kaybın oluştuğu birimin tespit ve değerlendirmeleri olarak sayılabilir. Tablo 8'de örnek bir operasyonel kayıp veri tabanı bilgi alanları ve bu alanların açıklamaları yer almaktadır[108].

[107] Murat Mazıbaş, "Bankalarda Operasyonel Risk Veri Tabanının Oluşturulması", **BDDK Çalışma Raporları,** Mart 2006, s.12.
[108] **Bankacılar Dergisi**, Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, "Operasyonel Risk Veri Tabanı", TBB, Nisan 2004, s.56.

Tablo 8:Operasyonel Kayıp Veri Tabanı Bilgi Alanları ve Açıklamaları

BİLGİ ALANI	AÇIKLAMA
Ref. No	İşlem referansı
Kayıt girişi yapan kişinin sicil no.su	İlk kayıt, düzeltme gibi her türlü giriş için ilgili kişi
Kayıt girişi yapan kişinin birimi/bölümü	İlk kayıt, düzeltme gibi her türlü giriş için ilgili bölüm
Onay Veren Bölüm / Kişi	Banka kendi yapısına uygun onay mercilerini tespit eder
Olayın Tanımı/Açıklaması	Olayın detayı serbest format yazılabilir.
Faaliyet Kolu	BDDK- işlevsel Faaliyet Listesi
Kayıp Kategorileri	BIS - Kayıp kategorileri dikkate alınır, Banka uygun görürse kendi alt tanımlarını oluşturabilir. Çoklu seçim yapılabilir.
Riskin Kaynağı	BIS - Risk kaynakları dikkate alınır, Banka uygun görürse kendi alt tanımlarını oluşturabilir. Çoklu seçim yapılabilir.
Kaybın Yeri	
Tarih Bilgileri	
Kaybın Nasıl Tespit Edildiği	Banka kendi yapısına uygun seçenekleri oluşturur.
Brüt Kayıp Tutarı (Tutar, Döviz Cinsi)	
Kayba ilişkin Tahsilat Bilgileri	Banka kendi yapısına uygun seçenekleri oluşturur.
Kaybın Muhasebeleştirme Tarihi	
Kaybın Kayıtlara Alındığı Hesap Skontu	
Olayın Direkt Etkisi	BIS - Kayıp türleri dikkate alınır, Banka uygun görürse kendi alt tanımlarını oluşturabilir. Çoklu seçim yapılabilir.
Olayın Maddi Olmayan Etkisi	Banka kendi yapısına uygun seçenekleri oluşturur, itibar ve strateji riskleri istenirse banka tarafından görüntülenebilir.
Olası Kayıp Bilgileri [Tutar, Açıklama)	Gerçekleşen kaybın yanı sıra henüz gerçekleşmemiş ve belki hiç gerçekleşmeyecek oluşması muhtemel diğer kayıplar
Olayın Durumu	
Denetime tabi olup, olmadığı (Evet(E)/ Hayır(H))	
Kontrol Eksiklikleri	Banka kendi yapısına uygun seçenekleri oluşturur.
Kaybın Soruşturrna /İnceleme/Dava Konusu Yapılıp Yapılmadığı	
Yönetimin Aldığı Kararlar/Tedbirler	Karşılaşılan riskin giderilmesi/azaltılması/kontrol edilmesine dönük bankanın vereceği kararlar
Kaybın Piyasa veya Kredi Riski ile Birleşik Opr. Riskten Kaynaklanıp Kaynaklanmadığı	

Kaynak: TBB, Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, **"Operasyonel Risk Veri Tabanı"**, Nisan 2004, s.56.

Bankalar veri modelinin oluşturulması ve veri tabanı sisteminin kurulması esnasında bir takım sorunlarla ve güçlüklerle karşılaşabileceklerdir. Bunlar verinin kalitesinden, toplanmasından ve uyumsuzluğundan kaynaklanabilir. Verinin toplanması aşamasında; kayıp olayının gizlenmesine ve raporlanmamasına yönelik saikler, veri toplama süreci konusundaki bilgi noksanlığı, risk kültürünün yerleşmemiş olması, veri toplama süreçlerinin ve sistemlerinin tasarımından kaynaklanan sorunlar, veri girişine yönelik olarak oluşturulan bilgi işlem sistemlerinin yetersizliği veya kullanışsızlığı gibi güçlükler yaşanabilir[109].

İçsel verilerin operasyonel risk ölçümü için yetersiz kalması nedeniyle dışsal verilere ihtiyaç ortaya çıkabilir. Dışsal verilerin risk ölçümünde kullanılmasında şu sorunlarla karşılaşabilinir[110]:

a) Dışsal verilerin farklı ölçeğe, kültürlere, risk alma eğilimine, kontrol yapılarına, süreçlerine ve faaliyet bileşimine sahip kuruluşlardan elde ediliyor olması bu verilerin spesifik bir banka açısından kullanışlılığını azaltmaktadır.

b) Kamuya açık kaynaklardan elde edilen operasyonel risk verileri birçok eksikliği ve sapmayı içerdiğinden doğrudan modelleme amaçlarına uygun değildir.

c) İçsel ve dışsal verilerin farklı dağılım özellikleri taşıması nedeniyle bu iki veri setinin doğrudan bir araya getirilmesi mümkün değildir.

d) Bazı bankalarda iç kontrol sistemi etkinliği ve aksiyon hızı çok yüksek olmasına karşın bazı bankalarda aynı etkinliğe sahip değildir. Bazı bankalarda operasyonel riskler yüksek risk grubunda olmasına rağmen bu riskler tüm bankalarda aynı olmayabilir. Bu durumda iç verinin dış veri ile benzetimi, beklenmeyen zararın olması gerektiğinden daha yüksek hesaplanması ile sonuçlanabilmektedir[111].

[109] Mazıbaş, "Bankalarda Operasyonel Risk Veri Tabanının Oluşturulması", s.13.
[110] Ali Samad Khan, **"Data Modeling",** Presentation in *How to Master and Quantify Operational Risk, The GARP Operational Risk Seminar,* 18-19 October 2001, London'dan Mazıbaş, "Bankalarda Operasyonel Risk Veri Tabanının Oluşturulması" s.16-17.
[111] Nurgül Chambers ve Atilla Çifter, "Operasyonel Risk Yönetiminde Zarar Dağılımları İle Gelişmiş Ölçüm Yaklaşımı Uygulaması", **Doğuş Üniversite Dergisi**, 8, (2), (2007), s.152.

İKİNCİ BÖLÜM

2. RİSK YÖNETİM STANDARTLARI VE OPERASYONEL RİSK YÖNETİM UYGULAMALARI

Operasyonel risk yönetiminde en önemli husus operasyonel riske neden olabilecek risk kaynaklarının belirlenerek bunları önleyecek aksiyonların alınmasıdır. Böylece söz konusu risklerin meydana gelmesi, alınan proaktif önlemlerle engellenmiş olacaktır. Aşağıda risk yönetimine ilişkin geliştirilen standartlardan bahsedildikten sonra operasyonel risk kaynağı olarak öngörülen insan, sistem, süreç ve dışsal faktörlerin her biri için olması gerekli uygulamalara değinilmiştir.

Operasyonel risk yönetiminde amaç, riskin temel iki boyutu üzerinde yoğunlaşmaktadır. Bilindiği gibi riskin bir boyutu gerçekleşme olasılığı olarak tanımlanırken diğer boyutu, yaratacağı etki düzeyidir. İşte operasyonel risklerin önlenmesindeki amaç aslında risklerin etkilerini azaltmak değil tekrarlanma olasılıklarını düşürmektir. Bu nedenle sık sık karşılaşılan ancak yaratacakları zarar potansiyeli düşük olan operasyonel risklerle mücadelede daha uygun bir yöntemdir. Ayrıca, zarar henüz ortaya çıkmadan risklere neden olan faktörler üzerinde yoğunlaşarak risklerden kaçınmayı hedef alması itibarıyla, riskin neden olabileceği zararın azaltılmasında kullanılan yöntemlere göre daha etkin görülmektedir. Operasyonel risklerin önlenmesinde; süreçlerin yeniden yapılandırılması, işlerin ve görev dağılımlarının yeniden planlanması, işlevsel otomasyon, insan kaynakları yönetimi, yolsuzluk olaylarının önlenmesi ve ortaya çıkarılması gibi yöntemler kullanılmaktadır.

En genel anlamıyla, çok iyi ve kapsamlı oluşturulmuş olan bir kurumsal operasyonel risk yönetimi politikası şunları içermelidir[112]. (i) Üst yönetimin konuya ilişkin verdiği destek başarının ön koşuludur. (ii) Operasyonel risk yönetimi, kuruma önemli ve doğrudan bir değer kazandıracak şekilde gerçekleştirilmelidir. Doğrudan değer olarak daha düşük sermaye yeterliliği oranına ulaşıp daha yüksek bir kaldıraç etkisiyle daha fazla gelir yaratma, risk yönetimi konusunda kurumda farkındalığın gelişmesi veya kayıplardaki azalma kastedilmektedir. (iii)Kurumsal motivasyonu artırmak için teşvik edici araçlar risk

[112] Moosa, s.217 ve Haubenstock, s.261.

yönetimi sürecine dahil edilmelidir. Örneğin, fayda-maliyet ilişkisine bağlı bir risk yönetim yaklaşımı kurumsal seviyede daha fazla dikkat çekecek ve operasyonel uygulanabilirliği artacaktır. (iv)Baştan sona tüm risk yönetimi sürecinde riskin tanımlanmasında, risk kategorilerinde ve temel risk göstergeleri arasında bir tutarlıklık sağlanmalıdır. (v)Risk yönetimi sürecinde, doğru personelin doğru yerde çalışması sağlanmalı, gerekli eğitim ve uygulama desteği sunulmalıdır. Bu süreçte personel yönetimine ve teknolojiye belirgin bir kaynak ayrılmalıdır. (vi)Tüm süreçler, ölçümler ve kontroller sürekli iyileştirmeye tabi tutulmalı ve işletilmelidir. (vii) Risk yönetimine ilişkin sonuçlar tüm birimler ile paylaşılmalıdır.

2.1. Risk Yönetimine İlişkin Geliştirilen Standartlar

Kurumlar risk yönetimi kapsamında maruz kalabilecekleri riskleri tanımlayarak bunların yaratacağı olumsuz etkileri ve olası kayıpları azaltmaya, kontrol altına almaya dönük çalışmalar yapmaktadırlar.

Bu çalışmalar kapsamında, risk yönetimine ilişkin farklı yöntemler, teknikler, süreçler ve metodolojiler geliştirilmiş ve bunlar risk yönetimi ana şemsiyesi altında toplanmıştır. Aslında, risk yönetimi kavramı içeriksel yönden iki farklı tabana oturmaktadır: bunlardan ilki "ticaret riski" olarak bilinen ve girişilen faaliyet ilgili olarak elde edilen, kar veya zarar doğuran işlemler ile yani parasal değerler ile açıklanırken diğeri "operasyonel risk" olarak tanımlanan ve bir kurumun operasyonel ve ticari hedeflerini, sorumluluklarını yerine getirirken maruz kaldığı belirsizlikleri ifade eder.

Bu anlamda, operasyonel risk yönetiminin kökeni inşaat sektöründe can güvenliğini sağlamaya dönük olarak alınan önlemlere kadar dayandırılabilir. Operasyonel riskin yönetimine ilişkin geliştirilmiş olan araçlar inşaat mühendisliğine kadar geri götürülebiliyor olsa da özellikle son yıllarda kurumsal altyapıda yaşanan dönüşüm ve değişimler risk yönetimine yönelik çalışmaların derinleşmesini sağlamıştır[113]. Hizmet sektörünün ekonomi içerisinde giderek daha yüksek bir değer oluşturması, emek yoğun üretimden, teknoloji yoğun üretim sistemlerine geçiş olması, gelişen sermaye piyasalarına

[113] T. Raz ve D. Hillson, "A Comparative Review of Risk Managemenet Standards", Risk Management: **An International Journal,** 7 (4), (2005), s.53-66.

bağlı olarak kurumsal yönetim yaklaşımlarının tesis edilmesi, değişen ve gelişen yasal mevzuatın zorlayıcı unsurları gibi etmenlerden dolayı risk yönetimi giderek daha fazla bir şekilde ön plana çıkmıştır. İşte bu gelişmeler ve etkenler neticesinde risk yönetimi konusunda çeşitli tür ve kapsamda çalışmalar yapılmış, seminerler ve forumlar düzenlenmiş ve çeşitli standart setleri oluşturulmuştur.

Risk yönetimi sürecine ilişkin olarak gerçekleştirilmiş olan teorik çerçevelerin temelinde genellikle Nobel Ödülü sahibi Herbert A. Simon'ın gerçekleştirmiş olduğu çalışmalar vardır. Simon, risk ve belirsizlik karşısında bireylerin ve kurumların karar verme sürecini üç ana safhaya ayırtmıştır[114]: öncelikle maruz kalınan riskler tanımlanmalı ve anlaşılmalı, daha sonra analiz edilmeli ve değerlendirilmeli ve en son olarak da riskler çeşitli araçlarla yönetilmelidir. Süreçler makro bir bakış açısıyla değerlendirildiğinde, risk yönetim sürecinin temel olarak "planlama", "analiz", "yönetim" ve "kontrol" aşamalarından oluştuğu görülmektedir.

Risk yönetiminin nasıl gerçekleştirilmesi gerektiği üzerine bir çok ulusal ve uluslararası yöntem ve yaklaşım geliştirilmiştir. Bu tür yaklaşımların ilki AS/NZS 4360 olarak adlandırılan ve ilk versiyonu 1995'te, ikinci versiyonu da 2004'te Avustralya ve Yeni Zelanda'da geliştirilmiş olan yaklaşımdır. Daha sonra 1997 yılında Kanada'da CAN/CSA-Q850 adlı bir standart ve 2000 yılında da İngiltere'de BS-6079-3 adlı bir başka standart geliştirilmiştir. Risk yönetimi konusunda ABD'de ise muhasebe ve denetim sektöründe faaliyet gösteren şirket ve düzenleyicilerin oluşturmuş olduğu bir komisyon olan COSO (The Committee of Sponsoring Organisations of the Treadway Commission) tarafından 2004 yılında uzun süren çalışmalar neticesinde *"COSO: Enterprise Risk Management - Integrated Framework"* yayınlanmıştır.

Bir kurumun operasyonları, stratejik hedefleri ve amaçları da içine alarak kurumsal seviyede operasyonel riskin yönetimine ilişkin olarak etkin bir risk yönetim setinin nasıl olması gerektiğine dair geliştirilmiş olan temel bazı standartlar, Tablo 9'da

[114] Patrick Mc Connel, "A Standards Based approach to Operational Risk Management", http://www.continuitycentral.com/ORStandards.pdf (14 Temmuz 2008), s.3.

özetlenmektedir.[115] Tablo'da yer alan standart setleri, risk yönetimine ilişkin öngördükleri süreçler ve bu süreçler kapsamında yerine getirilmesi gerekenler açısından yol haritaları itibariyle birbirlerine oldukça benzemektedirler. Standartların temel yapısı genelde benzer olmasına karşın, standartlar arasındaki farklılıklar "öz"le ilgili olmayıp sadece terminolojik ifadelerin farklılığından kaynaklanmaktadır. Aşağıda özellikle bu standartlardan en kapsamlı ve kabul görmüş olarak uygulananı: COSO'nun kurumsal risk yönetimi çerçevesi detaylı olarak açıklanmaktadır.

Tablo 9: Risk Yönetimine İlişkin Geliştirilmiş Olan Standartlar

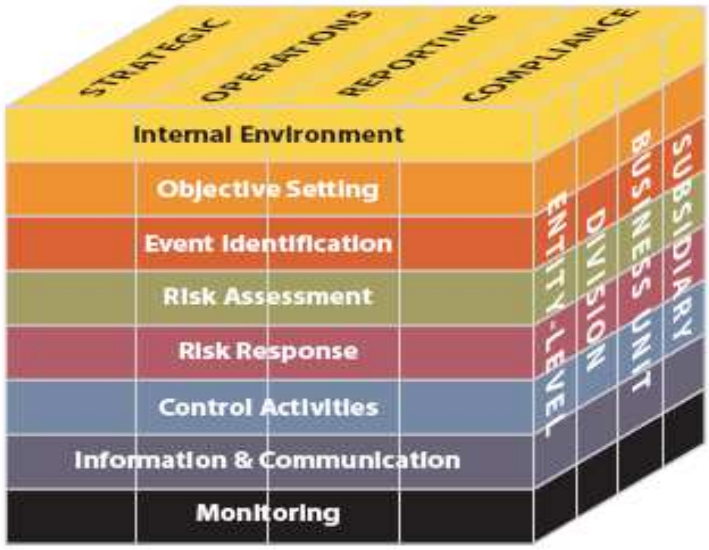
STANDARDIN İSMİ	YAYINLAYAN	YIL	Sayfa Sayısı
AS/NZS 4360:2004: / Risk Management	Standards Australia /Standards New Zealand	2004	28
CAN/CSA-Q850-97: Risk Management: Guideline for Decision-Makers	Canadian Standards Association (CSA)	1997	62
JIS Q2001:2001(E): Guidelines for Development and Implementation of Risk Management System	Japanese Standards Association	2001	20
COSO: Integrated-Entreprise Risk Management	The Committee of Sponsoring Organisations of the Treadway Commission	2004	125

Kaynak: RAZ, T. ve Hillson, D. **"A Comparative Review of Risk Managemenet Standards"**, Risk Management: An International Journal, 2005, 7 (4) , 53-66, s.3

[115] Söz konusu tablo -Raz, T. ve Hillson, D. "A Comparative Review of Risk Managemenet Standards", **Risk Management: An International Journal** 2005, 7 (4) ,53-66 s.3'den alınmıştır. Temel önceliği risk yönetimine sadece proje bazlı yaklaşan standartlar seti tabloya dahil edilmemiş, COSO ise tabloya sonradan eklenmiştir.

2.1.1. COSO Kurumsal Risk Yönetimi

Kurumsal Risk Yönetimi (KRY) birbiriyle ilişkili olan sekiz adet unsurdan oluşmaktadır. Bu unsurlar, kurumun faaliyetlerinden ortaya çıkmaktadır ve yönetimin verdiği kararlar ile de doğrudan ilişkilidir. Şekil 2'de yer alan COSO'nun baz aldığı sekiz katmanlı küpün her katmanı ayrı ayrı aşağıda açıklanmıştır[116]:



Şekil 2: Kurumsal Risk Yönetiminin Unsurları: COSO Metodolojisi
Kaynak: Committee of Sponsoring Organizations of the Treadway Commission (COSO). **"Enterprise Risk Management Integrated Framework, Executive Summary Framework".** New York, AICPA, September 2004, s.7.

2.1.1.1. Kurumsal Çevre (Internal Environment)

Kurumsal çevre, diğer tüm bileşenlerin temelini teşkil eder ve kurumun strateji ve hedeflerinin nasıl belirlendiğini, faaliyetlerin nasıl yapılandırıldığını, risklerin tanımlanmasını, değerlendirilmesini ve risklerle ilgili alınan tedbirlerin uygulamasını etkiler. Bunun yanında kurumsal risk yönetiminin kontrol faaliyetlerinde, bilgi, iletişim ve izleme faaliyetlerinin tasarımında ve etkin bir şekilde uygulanmasında önemli bir yeri vardır. Kurumsal çerçeve, kurumun etik değerleri, çalışanların yetkinliğine verilen önem, yönetimin

[116] Committee of Sponsoring Organizations of the Treadway Commission (COSO). "Enterprise Risk Management Integrated Framework, Executive Summary Framework", New York: AICPA, 2004, s.7.

çalışma biçimi, görevlerin ve sorumlulukların dağılımı gibi birçok faktörü bünyesinde barındırır.

Yönetim öncelikle riske yaklaşımını belirleyen risk felsefesini ve bu doğrultuda da risk toleransını tanımlar. Kurumsal çerçeve, kurumun riskleri ve bunlara ilişkin kontrol noktalarını nasıl tanımladığını ve bunları çalışanların nasıl değerlendirdiğini belirler. Kurumların en temel unsuru olan çalışanlar, içinde oldukları ortamdan etkilenmekte ve buna bağlı olarak da değerlerini, bireysel yeteneklerini, etik kurallara dönük bakış açılarını kurumun operasyonlarına yansıtmaktadırlar.

2.1.1.2. Hedefleri Belirleme (Objective Setting)

Kurumun hedeflerini gerçekleştirirken, kayıplara sebep olabilecek olayları kapsamlı bir şekilde değerlendirebilmesi için özelikle üst yönetimin operasyonel faaliyetleri, raporlaması ve yasal uyuma ilişkin amaçlarını da kapsayacak şekilde hedefleri belirlemesi gereklidir. Kurumun amaçlarına yönelik riskleri belirlemesi ve gerekli önlemleri alarak bunları yönetmesi için yönetimin önünde daha önceden belirlenmiş bir amaç setinin bulunması gereklidir. Bu bağlamda KRY, üst yönetimin kurumsal hedefleri belirlemesinde ve daha sonra da belirlenmiş olan hedeflerin kurumun misyonu ve risk toleransı doğrultusunda gerçekleştirilmesinde yönetime yardımcı olur.

2.1.1.3. Olay Tanımlama (Event Identification)

Yönetim, kurumsal stratejilerin uygulanmasını, amaç ve performans hedeflerine ulaşılmasını olumlu ya da olumsuz yönde etkileyebilecek içsel veya dışsal kaynaklı muhtemel olayların neler olduğunu belirlemelidir.

Bu aşamada, kurum söz konusu olayların kayba mı sebep olacağı, yoksa kuruma bir fırsat mı sunduğunu ya da her iki özelliği birden mi taşıdığını ayırt edebilmelidir. Potansiyel olarak olumsuz olaylar, işletme için risklere işaret eder ve söz konusu muhtemel olayların değerlendirilmesi ve önlenmesi ya da azaltılması için alternatif politikaların geliştirilmesi gerekir. Diğer taraftan potansiyel olarak olumlu olaylar, işletme için fırsatlar demektir ve yönetimin, söz konusu olayları stratejilerine ve hedef belirleme süreçlerine dahil etmesi beklenir.

2.1.1.4. Risk Değerlendirmesi (Risk Assessment)

Risk değerlendirme sürecinde, belirli bir dönemde kurumla ilgili olabilecek muhtemel olayların gerçekleşme olasılığı ve olası etkileri, nitel ya da nicel metotlar kullanılarak değerlendirilir. Tespit edilen risklerin, nasıl yönetilmeleri gerektiğini belirlemek için kapsamlı bir analiz yapılmalıdır. Riskler aynı zamanda etki edebilecekleri önceden belirlenmiş olan hedeflerle ilişkilendirilmeli ve risklerin etkisi ve alınan aksiyon sonrası geriye kalan riskler gerçekleşme ve etki düzeyleriyle beraber değerlendirilmelidir.

2.1.1.5. Riski Karşılama (Risk Response)

Yönetim, risk değerlendirmesi sonrasında fayda-maliyet analizi çerçevesinde risklere nasıl bir tepki verileceğini, yani risklerin nasıl yönetileceğini kararlaştırır. Burada risklerin muhtemel etkileri ile alınacak alternatif önlemlerin olası maliyetleri karşılaştırılır. Kurum çalışanları da günlük operasyonel faaliyetleri kapsamında, üst yönetim tarafından kurumun risk toleransı ve toleransına göre belirlenmiş risk yönetim politikalar doğrultusunda karşılaştıkları riskleri kabul etme, azaltma, paylaşma ya da riskten kaçınma şeklinde farklı aksiyonlar geliştirirler.

Kurum çapında riskler tanımlanıp, ölçüldükten ve değerlendirildikten sonra sıra alınacak aksiyonlara gelir. Riskin yarattığı etki seviyesi, gerçekleşme sıklığı, kurumun risk toleransı alınacak aksiyonun belirleyicisi olmaktadır. Alınacak aksiyonlar; riski kabullenmek, riskten kaçınmak, riski transfer etmek veya riski azaltmak şeklinde sıralanabilir. Şekil 3'den de görüleceği üzere gerçekleşme olasılığı ve şiddeti yüksek riskler için riskten kaçınma, gerçekleşme olasılığı yüksek ama şiddeti düşük riskler için riskleri azaltıcı, olasılığı düşük, şiddeti yüksek riskler için risklerin transfer edilmesi, olasılığı ve şiddeti düşük risklerin ise kabullenilmesi yönünde aksiyon alınması önerilmektedir[117]. Haritanın ortasındaki alana denk düşen riskler içinse alınacak aksiyonu kurumun risk toleransı belirlemektedir.

[117] Moosa, s.214.

Şekil 3: Alınacak Aksiyonları Gösteren Risk Haritası
Kaynak: Imad A Moosa, **"Operational Risk Management"**, Palgrave Macmillan, 2007, s.214.

2.1.1.5.1. Riskten Kaçınmak (Risk Avoidance)

Riskten kaçınmak olarak adlandırılan tercih, her zaman uygulanabilirliği olan sonuçlar üretmemektedir. Çünkü riskin doğmasını engelleyecek "en etkili" çözüm, işleri tamamen durdurmaktır ki bu kurumsal anlamda pek mantıklı bir tercih değildir. Ama bütünleşik olarak faaliyet gösteren bazı kurumlar, eğer faaliyet gösterdikleri belirli alanlarda daha fazla riske maruz kalıyorlarsa ve söz konusu faaliyetlerini kurum dışından tedarik ederek de yerine getirebiliyorlarsa, riskten kaçınmak anlamında bazı iş ve faaliyet birimleri durdurularak dışarıdan hizmet temini yolu seçilebilir. Böylelikle, firma rekabet avantajına sahip olduğu alanda yatırımlarına devam ederek pozisyonunu daha da güçlendirebilir[118].

2.1.1.5.2. Riski Azaltmak (Risk Reduction)

Bir başka alternatif ise, kontrol faaliyetlerinin gözden geçirilmesi ve yeni kontrol noktalarının tesis edilerek riskin azaltılması yöntemidir. Süreçleri yeniden tasarlamak, personele eğitim sağlamak veya teknik bazı önemler getirmek riski azaltmak çerçevesinde değerlendirilebilir ve fayda maliyet analizleri kararlarının oluşturulmasında kullanılabilir. Dolayısıyla, riski azaltmanın maliyeti ve getirisi arasındaki ilişki riski azaltma politikası

[118] Robert Hübner, Mark Laycock&Fred Peemöller, "Managing Operational Risk", **"Advances in Operational Risk Firm-wide Issues for Financial Institutions"**, London: Risk Boks, 2001, s.12.

kapsamında da değerlendirilir. Risk azaltma politikaları, tespit edilen ve ölçülen riskleri kurumun riski toleransı doğrultusunda oluşturulmuş olan kabul edilebilir seviyelere indirmeyi hedefler.

Risklerin azaltılmasına yönelik aksiyon kısaca risk haritası üzerinde ifade edilecek olursa, kurumsal risk toleransının ve kabul edilebilir seviyenin dışındaki alanda bulunan risklerin gerekli kontrollerin tesisi ile kabul edilebilir seviyelere indirilmesi olarak tanımlanabilir.

2.1.1.5.3. Risk Paylaşımı/Transferi (Risk Sharing/Transfer)

Risk transferi ya da risk paylaşımı olarak da ifade edilen kavram ise, riskin gerçekleşme olasılığını veya riskin gerçekleşmesi durumunda etkilerini azaltmak için riskin bir kısmını bir başka tarafla paylaşarak/transfer ederek, kurum dışı bir çözüm oluşturmaktır.

Riski paylaşma yöntemleri olarak en çok görülenler: Sigorta yapılması, risk havuzları oluşturulması, kurum içinde gerçekleştirilen riskli sayılabilecek hizmetlerin veya üretilen ürünlerin dışarıdan satın alınmasıdır. Sigorta özellikle ortaya çıkma sıklığı az ancak neden olduğu zarar miktarı yüksek olan olaylar için tercih edilmektedir. Bankalarca en yaygın olarak kullanılan sigorta ürünlerinin başında “Banker’s Blanket Bond” poliçesi olmak üzere, “Yönetici ve Çalışan Yükümlülükleri”, “İstihdam Uygulamaları Yükümlülükleri” ve “Mesleki Yükümlülükler” poliçeleri gelmektedir[119].

Böylelikle, işletmelerin mali tablolarında yer alacak olan operasyonel risk kaynaklı olabilecek karşılıklar bir ölçüde azaltılarak sigorta şirketlerine transfer edilmiş olacaktır. Bu türdeki risk yönetim enstrümanları son yıllarda operasyonel riskin giderek daha fazla önem kazanmasına bağlı olarak artmaktadır[120]. Diğer taraftan ise sigortalamaya bağlı olarak risk transferinin ne ölçüde gerçekleştirildiği de önemli bir soru işareti olarak durmaktadır. Çünkü sigorta sadece riskin gerçekleşmesi durumunda sigorta ettiren kuruma belirli bir finansal

[119] Risk yöneticileri Derneği Bülteni, “Operasyonel Risklerin Kontrol Edilmesi ve/veya Azaltılmasına Yönelik Faaliyetler”, Eylül 2004, s.5.
[120] Cruz, s.258.

güvence sağlamasına karşın sigorta ettiren kurum mali olmayan konulardan dolayı operasyonel riskin sonuçlarıyla yine karşı karşıyadır[121.]

Kurumlar sigortalama tercihi dışında bazı hizmet ya da ürünlerini kurum dışından temin ederek de belirli ölçüde risk transferini gerçekleştirmiş olurlar. Dışarıdan hizmet alımında, kurumlar ana faaliyet konusu olmayan bazı ürün ve hizmetleri bu tür ürün ve hizmetlerin üretiminde uzmanlaşmış ve maliyet etkin çalışan kurumlardan temin ederek hem maliyetlerini azaltabilirler hem de üstlenmiş oldukları bazı risklerden belirli ölçüde kurtulabilirler. Kurumlar, bilgi sistemlerinde ya da insan kaynaklarında bu tür dışarıdan hizmet alımlarını gerçekleştirebilirler. Dışarıdan hizmet alımının bazı temel faydaları kısaca şu şekilde sıralanabilir[122]: maliyetlerin data etkin şekilde kontrol altına alınması, faaliyet gösterilen konuya odaklanıp en iyi ve en etkin hizmetin sunulması, ana faaliyet konusunu oluşturmayan alanlar ile uğraşılmadığı için sermayenin daha etkin ve verimli kullanılabileceği alt yapının sağlanması ve kurum içi bürokrasi ve kırtasiyeciliğin azalmasıdır.

2.1.1.5.4. Riski Kabul Etmek (Risk Acceptance)

Riski üstlenmek ise, riskten kaçınmanın tam tersidir. Olağan iş hayatında, bir kurum yukarıda bahsedilen araçları bütüncül bir şekilde kullanmaktadır. Böylelikle, kurum riski azaltıcı kontroller geliştirdikten sonra ve belli ölçüde riskin maliyetini sigortaladıktan sonra kalan kısmı üstlenmektedir. Kurum, gerçekleşme olasılığı ve etki düzeyi yüksek risklerden kaçınırken, gerçekleşme olasılığı ve etki düzeyi düşük olan riskleri ise üstlenmekte, gerçekleşme olasılığı düşük ama etki düzeyi şiddetli olan riskleri transfer etmektedir.

2.1.1.6. Kontrol Faaliyetleri (Control Activities)

Kontrol faaliyetleri, kurumun maruz kaldığı risklere karşı yönetim tarafından alınan aksiyonların (riski azaltmak, riskten kaçınmak, riski kabul etmek, riski paylaşmak) gerçekleştirilmesini temin eden politika, prosedür, kurallar ve uygulamalardan

[121] Moosa, s.212.
[122] P. Mestchian, "Operational Risk Management: The Solution is in the Problem, in Advances in Operational Risk: Firm-Wide Issues for Financial Institutions, London:Risk Boks, 2003'den Moosa, s.213.

oluşmaktadır. Bu faaliyetler özellikle her bir kontrol hedefine yönelik olarak, belirlenen riskleri azaltmak amacıyla düzenlenir. Kontrol tedbirlerini almak ve kontrol faaliyetlerini yürütmek idari bir görev ve sorumluluktur. Başta üst yöneticiler olmak üzere, bütün personel, kurumlarının amaçlarına ulaşılmasını önleyecek unsurlara ve risklere karşı duyarlı olmak durumdadır.

Söz konusu kontrol faaliyetleri; yetkilendirme, onay, doğrulama, mutabakat, operasyonel performansın takibi, varlıkların güvenliğinin ve görevler ayrılığının sağlanması gibi çeşitli kontrol araçlarıyla kurumun tüm birimleri ve tüm süreçlerini kapsayacak şekilde kurum çapında yürütülür.

Görevler ayrılığı ilkesi ile görev ve yetkilerin aynı kişide birleşmesinin önlenmesi, belli işler için onay ve doğrulama yapılması, muvafakat aranması, işlemlerin kayıt altına alınması, fiziki sayımlar ve mutabakat işlemleri, operasyonel performansın takibi, varlıkların güvenliğinin sağlanması gibi çeşitli kontrol teknikleriyle kurumun tüm birimleri ve tüm süreçlerini kapsayacak şekilde kurum çapında kontrol faaliyetleri yürütülür.

2.1.1.7. Bilgi ve İletişim (Information and Communication)

Risk yönetimi kapsamında gerekli olan bilgiler çalışanların sorumluklarını daha iyi yerine getirebilmeleri için derlenir ve ilgililerine belirlenmiş bir periyotta ve şekilde iletilir. Kurum çalışanlarının, risk yönetimini en etkin şekilde sürdürebilmeleri için risklerin tespit edilmesi, değerlendirilmesi ve gerekli aksiyonların alınması konusunda bilgi akışının sağlanması gerekmektedir. Kurum içi etkin iletişim de geniş anlamıyla, kurum içinde birimler arasında yatay ve dikey olarak gerçekleşmeli ve çalışanlar da görev ve sorumluluklarını net bir şekilde bilmelidirler.

2.1.1.8. Gözetim/ İzleme (Monitoring)

Kurumsal risk yönetiminin etkin bir şekilde işleyip işlemediğinin belirlenmesi için risk yönetimi sürecinin performans kalitesinin değerlendirilmesi gerekir. İzleme; sürekli izleme faaliyetleri, bağımsız izleme faaliyetleri veya her ikisinin bileşiminden oluşan izleme faaliyetleriyle yerine getirilir. KRY'nin işleyişi detaylı bir şekilde değerlendirilir ve gerektiği

zaman bazı değişiklikler yapılabilir. Böylelikle, KRY dinamik bir yaklaşım olup, şartlara göre değişiklik yapılabilir.

Sürekli izleme faaliyetleri, kurum faaliyetlerinin normal işleyişi içinde faaliyetle birlikte eş zamanlı olarak gerçekleştiği için bağımsız izleme faaliyetlerinden daha etkindir. Bağımsız izleme, işlem sona erdikten sonra yapıldığı için problemlerin sürekli izleme faaliyetleri aracılığıyla tespit edilmesi daha kolaydır.

KRY, risklerin değerlendirilmesiyle riskler karşısında nasıl aksiyon alınacağının belirlenmesine ve kontrol faaliyetlerinin içeriğinin ve şeklinin oluşturulmasına, kurum içi bilgi akışı ve iletişimin yeniden gözden geçirilmesine, üst yönetimin gerçekleştirdiği gözetim etkinliklerinin revize edilmesine kadar farklı unsurları etkileyen dinamik bir süreçtir. Böylelikle, KRY bir parçanın sadece kendinden sonraki geleni etkilediği şeklinde tanımlanan tek yönlü bir süreç olmayıp, her bir parçanın diğer unsurları da etkilediği çok boyutlu, kendini tekrarlayan bir süreçtir.

KRY, kuruma özgü özelliklerden, faaliyet gösterilen sektörden, kurumun sektör içindeki yerinden, kurumun faaliyetlerinin hacminden ve riskin kurumsal olarak nasıl tanımlandığından etkilendiğinden dolayı tüm kurumlarda aynı şekilde uygulanamaz. Diğer bir ifadeyle, tüm kurumların KRY'nin temel unsurları olarak yukarıda sayılan parçaları kendi yönetim anlayışları içinde oluşturmaları gerekli olsa da, çalışanların görev ve sorumluluklarının belirlenmesi, risk yönetimi sürecinde kullanılacak olan yöntem ve yaklaşımlar gibi risk yönetimi unsurlarının şirketler tarafından uygulanması şirketten şirkete bazı farklılıklar gösterebilir.

2.1.2. Bilgi Sistemleri İçin Geliştirilen Standartlar

Bilgi teknolojileri (BT) yönetiminin etkinliği, teknolojik gelişmelere paralel olarak giderek daha fazla önem kazanmakta ve bu durum da kurumların BT'ye yönelik sektördeki en iyi uygulamaları kullanmak istemeleri hedefini ortaya çıkarmaktadır. Bu çerçevede, kurumların BT'ye dönük yatırım kararlarını yeniden şekillendiren birçok neden vardır[123.] Öncelikle, kurumlar BT' ye yapmış oldukları yatırımlar dolayısıyla daha fazla değer elde

[123] ITGI ve OGC, "Aligning COBIT, ITIL and ISO 17799 for Business Benefits: Managmeent Summary", 2005, http://www.itgovernance.co.uk/files/ITIL-COBIT-ISO17799, (03 Temmuz 2007), s.7.

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 (Sarbanes-Oxley Yasası gibi) kurumların BT yatırımlarının niceliğine ve niteliğine dönük bakış açılarını etkilemiştir.

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. 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 yürütüyor olması, "en iyi uygulama örneklerinin" kurumsal BT risk yönetimi işleyişinde uygulanıyor olmasıyla kurumsal verimlik artacak, daha az operasyonel hata gerçekleşecek, düzenleyiciler ve birlikte iş yapılan tarafların kuruma karşı sahip oldukları güven duygusu artacaktır.

Dolayısıyla, tutarlı ve istikrarlı bir bilgi işlem 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 yönetim 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.

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.

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.

BT risk yönetimine ilişkin olarak geliştirilmiş olan çeşitli standartların ilki İngiltere tarafından geliştirilmiştir. İngiltere hükümeti, BT'ye dönük en iyi uygulama 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 yönetim standardıdır. BT Güvenlik Uygulama Rehberi (IT Security Code of Practice) olarak oluşturulmuştur[124].

BS 7799-2 standardı ilk olarak 1999 yılında BSI(British Standarts Institution) tarafından bilgi güvenlik yönetim 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 yönetim 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

[124] Kemal Özmen, **"Bilgi İşlem Risk Yönetimi"**, http://www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=279 (21 Mayıs 2008), s.3.

önlemler ISO 27002 standardında, önlemlerin nasıl yaşatılacağı ise ISO 27001 standardında açıklanmaktadır[125].

COBIT (Control Objectives for Information and Related Technology) metodolojisi ISACA tarafından geliştirilmiştir ve 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 yönetim süreçleri üzerine tesis edilen bir BT kontrol çerçevesi olarak geliştirilmiştir[126].

Aşağıda bilgi sistemleri kapsamında geliştirilmiş olan bu standart ve kontrol çerçevelerinden özellikle BDDK'nın Bankalar için getirdiği bir düzenleme olan COBIT metodolojisi ve operasyonel riskin sistem tarafını ilgilendiren bilgi güvenliğinin sağlanmasına yönelik önlemleri sıralayan ISO 27001 standardı açıklanacaktır.

2.1.2.1. COBIT Metodolojisi

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

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

[125] Burak Bayoğlu, **Bilgi Güvenliği Yönetim Sistemi Uygulama ve Denetleme Semineri Notları**, Takasbank (Aralık 2008), TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, s.73.
[126] ITGI ve OGC, **"Aligning COBIT,ITIL, and ISO 17799 for Business Benefits:Management Summary"**, 2005, http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf (19 Haziran 2008), s.9.

yapılmasını temin etmek için oluşturulmuş olan bir kontrol hedefler çerçevesidir[127]. 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, SOx ve Basel II gibi uluslararası düzenlemelerle uyumun sağlandığını gösteren bir çerçeve sunarak kontrol hedefleri, teknik gereksinimler, ticari riskler ve performans ölçümleri arasındaki ilişkiyi sağlar[128]. COBIT'in iş odaklı bir yaklaşımının olması kurumun ticari hedefleriyle BT hedeflerini uyumlu hale getirmesine, bu hedeflerin gerçekleşip gerçekleşmediğini ölçmeye dönük çeşitli ölçüt ve olgunluk modellerini içermesine ve sorumlulukları da BT ve BT dışı süreçlerin sahiplerine vermesine bağlıdır. Dolayısıyla COBIT, BT yönetiminin ticari yaklaşımlarla uyumlu olmasını, kaynakların en verimli şekilde kullanılmasını, risklerin en etkin bir şekilde yönetilmesini sağlayan bir çerçeve sunarak BT risk yönetimini oluşturur.

COBIT bir kurumda BT risklerinin etkin bir şekilde yönetilmesine ilişkin olarak daha çok ne yapılması gerektiğini açıklarken nasıl yönetilmesi gerektiği üzerinde fazla durmaz[129]. 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[130].

COBIT, temel olarak üç gruba seslenir[131]:

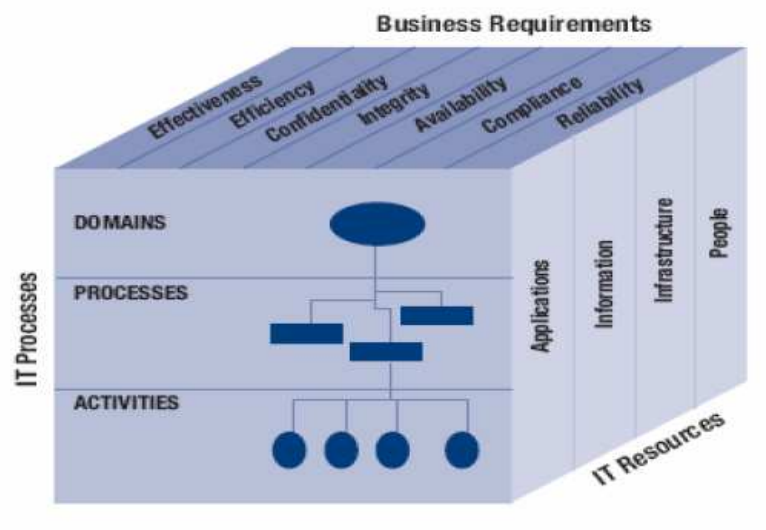
- BT'ye dönük risk ve kontrolleri dengelemek isteyen üst yöneticilere,
- Kurum içi ve kurum dışı müşterilere karşı verilen hizmetleri gerçekleştirirken üzerinde çalıştıkları bilgi sistemlerinin güvenlik ve kontrolünün yeterli olduğuna dair emin olmak isteyen çalışanlara,

---

[127] Elize Natasa Artinyan, " COBIT Çerçevesi", **Active Dergisi**, Sayı.54, 2007, s.1.
[128] Edouard Drougou, "IT Governance at a Financial Institution", **(Yayınlanmamış Master Thesis, KTH Electirical Engineering, Stockholm)**, s.35.
[129] ITGI ve OGC, **"Aligning COBIT,ITIL, and ISO 17799 for Business Benefits:Management Summary"**, 2005, http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf (19 Haziran 2008), s.10.
[130] GTAG, "**Bilgi Teknolojisi Kontrolleri**", Uluslararası İç Denetim Ensitütüsü, http://www.tide.org.tr/tideweb/resimler/upload/Documents/GTAG, (16 Haziran 2008), s.99.
[131] Mathias Salle, "**IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing**" HP Laboraitories Palo Alto, 2004, s.4. http://www.hpl.hp.com/techreports/2004/HPL-2004-98.html (14 Ağustos 2008).

- Üst yönetime kurum içi kontrollerin etkinliğine ilişkin olarak rapor düzenleyen ve düzenlediği raporları desteklemek amacıyla denetçilere.

COBIT kontrol çerçevesini; BT kaynakları (IT Resources), BT süreçleri (IT Processes) ve BT bilgi türleri (Business Requirements) olmak üzere üç boyutlu bir yapıda ele almaktadır ve bu üç boyutun altında yer alan unsurlar Şekil 4'deki COBIT küpünde gösterilmektedir[132].



Şekil 4: COBIT Küpü

Kaynak: Robert Moller, "**Brink's Modern Internal Auditing**", John Wiley, 2005, New Jersey, s.147-148.

Küpün sağ tarafı BT kaynakları olarak ifade edilir. COBIT BT kaynaklarının verimliliğini maksimum yapmaya çalışır. BT Kaynakları;

- **Uygulamalar (Applications),** bilgiyi işleyen otomatik kullanıcı sistemler ve yazılı prosedürler.
- **Bilgi (Information)**, bilgi sistemlerine girdi olarak giren, işlenen ve sistemlerden çıktı olarak çıkan veri.

[132] Robert Moller, **Brink's Modern Internal Auditing**, New Jersey:John Willey, 2005, s.147-148.

- **Altyapı (Infrastructure)**, uygulamaların işlemesine yardımcı olan donanım, işletim sistemi, ağ sistemleri gibi teknoloji ve yöntemler.
- **İnsan (People)**, bilgi sistemlerini ve servislerini planlayan, sistemlerin elde edilmesini sağlayan, destek veren, izleyen ve değerlendiren personel.

Yukarıda sayılan 4 grup altında toplanan ve kontrolü ve yönetimi gerek tek tek gerekse de grup halinde gerçekleştirilmesi gereken kurumsal varlıkları gösterir. Yani, bir kurumda kullanılan sadece yazılımlar ve ağ değil aynı zamanda, kullanılan teknoloji, bu uygulamaları gerçekleştiren personel (insan) ve diğer BT varlıklarını destekleyen unsurlar da beraber incelenmelidir. COBIT kontrol çerçevesinin uygulamasına küpün sağ tarafından başlanmış olsa da, kontrole dönük incelemeler küpü oluşturan diğer parçalarla entegre bir biçimde ele alınmalıdır.

COBIT küpünün, ikinci boyutunu ise aşağıda belirtilen 4 alan (domains) içerisinde toplam 34 süreç (process) ve 318 detaylı kontrol hedefi (detailed control objectives) oluşturmaktadır.

1) Planlama ve Organize Etme (PO:Plan and Organize)
2) Elde Etme ve Uygulama (AI:Acquire and Implement)
3) Servis Sağlama ve Destek (DS:Deliver and Support)
4) İzleme ve Değerlendirme (ME:Monitor and Evaluate)

Küpün üçüncü yüzünü oluşturan BT bilgi kriterlerinde süreçler kalite, *fiduciary* ve güvenlik açılarından üç şekilde tasnif edilir ve tüm BT sistemleri ve süreçleri bu üç kritere bağlı olarak değerlendirilmelidir. Kalite tanım altında BT süreçlerin genel kalitesine ve niteliksel yeterliliğine dönük tespitleri, *fiduciary* tanımı altında muhasebe ve finansal kontrollere dönük tespitleri ve güvenlik tanımı altında da BT kaynaklarıyla ilişkili kontrol ve güvenliğe ilişkin tespitler yer alır. BT süreçleri aşağıda yer alan tanımlar doğrultusunda değerlendirilir ve birincil ya da ikincil kontrol hedefi olarak sınıflandırılır. Bunlar aşağıda belirtilen 7 kısımdan oluşmaktadır:

- ✓ **Etkin (Effectiveness):**İş sürecine uygun, zamanında, doğru, tutarlı olarak sağlanan bilgi
- ✓ **Verimlilik (Efficiency):** Kaynakların optimum kullanılması
- ✓ **Gizlilik (Confidentiality):** Hassas bilginin yetkisiz erişimlere karşı korunması

- ✓ **Bütünlük (Integrity):**Bilginin doğruluğu ve eksiksiz olması
- ✓ **Süreklilik (Availability):** Bilginin ihtiyaç olunduğunda erişebilir olması
- ✓ **Uyumluluk (Compliance):** Kanunlara düzenlemeler ve sözleşmelere uyumluluk
- ✓ **Güvenilirlik (Reliability):** Kişi veya sistemin fonksiyonlarını beklenmedik olaylara veya kötü niyetli hareketlere rağmen doğru gerçekleştirmesi.

Planlama ve Organize Etme: Bu alan, iş birimleri ile bilgi işlem birimlerinin eşgüdümünün sağlanması, kurumun hedeflerine varabilmesi için bilgi teknolojilerini ne şekilde kullanabileceğini, bu teknolojilerin kullanımından azami faydanın sağlanabilmesi için tesis edilmesi gereken organizasyon ve altyapıyı, bilgi sistemleri kaynaklı risklerin yönetimini ve bilgi sistemlerinin kalite ve performans ölçümlerini inceleyen aşağıda sıralanan 10 adet kontrol hedefinden oluşur;

PO1 : Stratejik BT Planının Tanımlanması
PO2 : Bilgi Mimarisinin Tanımlanması
PO3 : Teknolojik Yönün Belirlenmesi
PO4 : BT Organizasyon ve İlişkilerinin Tanımlanması
PO5 : BT Yatırımlarının Yönetimi
PO6 : Yönetimin Hedeflerinin ve Talimatlarının İletilmesi
PO8 : Kalite Yönetimi
PO7 : İnsan Kaynakları Yönetimi
PO9 : Risk Değerlendirme ve Yönetimi
PO10: Proje Yönetimi

Elde Etme ve Uygulama: Bu alan, bilgi sistemlerine ilişkin gereksinimlerin belirlenmesi, gerekli teknolojinin tedarik edilmesi, kurum dahilinde hayata geçirilmesi, kullanıcı eğitimleri, destek süreçleri, kuruma ait varlıkların bakım planlarının hazırlanması, değişiklik yönetimi gibi aşağıda sıralanan 7 adet kontrol hedefinden oluşur;

AI1 : Otomasyon Çözümlerinin Belirlenmesi,
AI2 : Uygulama Yazılımı Tedarik Edilmesi ve Bakımı,
AI3 : Teknoloji Altyapısının Tedarik Edilmesi ve Bakımı,
AI4 : İş ve Kullanımın Etkin Kılınması,
AI5 : BT Kaynaklarının Sağlanması,
AI6 : Değişiklik Yönetimi,
AI7 : Çözüm ve Değişikliklerin Kurulması ve Kabul Edilmesi

Servis Sağlama ve Destek: Bu alan, bilgi sistemlerine ilişkin hizmetlerin sürekliliğinin sağlanması, bu faaliyetlerin iş birimlerinin hedefleri ile uyumunun korunması, güvenlik ve eğitim süreçleri gibi 13 adet kontrol hedefinden oluşur;

DS1 : Hizmet Düzeyi Belirleme ve Yönetimi
DS2 : Üçüncü Parti Hizmet Yönetimi
DS3 : Performans ve Kapasite Yönetimi
DS4 : Sürekli Hizmetin Sağlanması
DS5 : Sistem Güvenliğinin Sağlanması
DS6 : Harcamaların Belirlenmesi ve Bütçelenmesi
DS7 : Kullanıcı Eğitimi
DS8 : Kullanıcılara Yardım ve Danışmanlık
DS9 : Konfigürasyon Yönetimi
DS10 : Problem ve Olay Yönetimi
DS11 : Veri Yönetimi
DS12 : Fiziksel Çevre Yönetimi
DS13 : Operasyon Yönetimi

İzleme ve Değerlendirme: Tüm BT süreçleri düzenli olarak kalite ve uyum yönünden periyodik olarak gözden geçirilip değerlendirilmelidir. Böylelikle, üst yönetimin kurumun sahip olduğu kontrol süreçleri hakkında bilgisi olacağı gibi iç ve dış denetimler çerçevesinde elde edilen bağımsız değerlendirmeler de bu alanda yer alır. Söz konusu alan 4 adet kontrol hedefinden oluşmaktadır.

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

Bu yukarıda açıklana dört ana bölümün oluşturduğu yapı, bilginin bütün yönlerini ve bunu destekleyen teknolojileri kapsar. Bu 34 adet üst-seviye kontrol hedeflerini dikkate alarak, iş süreci sahibi, IT ortamı için uygun ve yeterli bir kontrol sisteminin kurulmasını sağlayabilir.

2.1.2.2. ISO/IEC 27001

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler standardı bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) (Information Security Management System - ISMS) kurmak isteyen kuruluşun risk analizi çalışmasının ardından çeşitli kontrollerin uygulanarak mevcut risklerin yönetimi için kullanılan bir standarttır. Bu standart BGYS'ni kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için hazırlanmıştır. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri standardı çerçevesinde yapılması gereken hususlar aşağıda detaylı olarak incelenmiştir.

2.1.2.2.1. Bilgi Güvenliği Politikası

Kurumda üst yönetim tarafından onaylanmış üst yönetimin bilgi güvenliği yönetimi ile ilgili taahhüdünü ve kurumsal yaklaşımı yansıtan ve tüm çalışanlarca da bilinen bir bilgi güvenliği politikası olmalıdır. Kurumda bilgi güvenliği politikasının geliştirilmesi, değerlendirilmesi ve tanımlanmış bir süreç eşliğinde gözden geçirilmesinden sorumlu bir sahibi olmalıdır. Politika sahibinin sorumlulukları yönetim tarafından onaylanmalı ve politikanın gözden geçirme süreci belli bir prosedür doğrultusunda yapılmalıdır. Bu kapsamda bilgi güvenliği ile ilgili önemli değişiklikler, bilgi güvenliğine kurumsal yaklaşım, uygulanan kontroller takip edilmeli, bilgi güvenliği için kaynak ayrılması ve sorumluların atanması konularında iyileşme sağlanmalıdır.

2.1.2.2.2. Bilgi Güvenliği Organizasyonu

Kurumda bilgi güvenlik organizasyonu kurulmalıdır. Bunun kurulmasında yönetimin aktif desteği, bilgi güvenliliği ile ilgili hedeflerin belirlenmesi, kurumun taahhütte bulunması ve sorumluların atanması ile sağlanabilir. Kurumdaki BT güvenlik süreçlerinin yürütülmesinden sorumlu "Bilgi Güvenliği Sorumluları" olmalıdır.

Kuruma alınacak yeni BT varlıklarına ilişkin olarak bunların kullanım amacı, şekli, mevcut güvenlik politikalarıyla ve güvenlik ihtiyaçları ile uyumu incelenmeli ve yönetimin onayından geçirilmelidir. Kurumun bilgi varlıklarını korumak için yapmak zorunda olduğu gizlilik anlaşmaları ile ilgili ihtiyaçları açık olarak tanımlanmalı ve gözden geçirilmelidir. Gizlilik anlaşmaları bilginin yasal yollarla korunması için gerekli şartları içermelidir.

Kurumun herhangi bir acil durumda emniyet, itfaiye vb. kuruluşlarla kimin ne zaman irtibat kuracağını ve olayın nasıl rapor edileceğini tarif eden bir prosedürü olmalıdır.

Kurumda mevcut uygulamaların güvenlik politikası esasları doğrultusunda yürütüldüğü, güvenlik politikasının etkinliği ve uygulanabilirliği düzenli bir şekilde bağımsız bir kurum veya kuruluş veya kurum içinden bağımsız bir denetçi aracılığıyla denetlenmeli ve denetimin sonuçları kaydedilip yönetime bildirilmelidir.

Kurumun bilgi sistemlerine erişen üçüncü taraflarla ilgili olarak da bir takım düzenlemelerin yapılması bilgi güvenliği açısından önem taşımaktadır. Üçüncü tarafın kuruma ait bilgi veya bilgi işlem araçları ile ilgili erişim, işlem veya iletişimi ile ilgili düzenlemeler yapan sözleşmelerde kurumun güvenlik ihtiyaçları karşılanmalıdır. Bilgi sistemlerine üçüncü tarafların erişiminden kaynaklanacak riskler belirlenip erişim hakkı verilmeden önce bununla ilgili tedbirler alınmalıdır. Kurum içerisinde görevlendirilmiş üçüncü parti çalışanlar için riskler belirlenmiş ve uygun kontroller tesis edilmiş olmalıdır. Müşterilere kurumun BT varlıklarına erişme hakkı verilmeden önce güvenlik ihtiyaçları ile ilgili tedbirler alınmalıdır.

2.1.2.2.3. İnsan Kaynakları Güvenliği

2.1.2.2.3.1. İşe Almadan Önce

Kurumun bilgi güvenliği politikası uyarınca iş başvurularında, işe alınacak personel için doğrulama testleri yapılmalıdır. Doğrulama testleri adayın özgeçmişinde beyan edilen akademik ya da profesyonel vasıfların doğruluğunu içeren bir istihbarat çalışmasıdır. İşe alınacak personelin görevleri, yetkileri ve sorumluluklarının açıkça tanımlanmış ve işe alınmadan evvel aday tarafından iyice anlaşılmış olması sağlanmalıdır.

2.1.2.2.3.2. Çalışma Sırasında

Kurum personeline ve kurumun BT varlıklarına erişim yetkisi bulunan üçüncü parti kullanıcılara bilgi güvenliği ile ilgili eğitimler verilmeli, mevcut politika ve prosedürlerin gerektirdiği güvenlik tedbirleri ve kurallar bütünü anlatılmalı, bunlara uyulmaması durumunda devreye girecek cezai yaptırımlar açıklanmalıdır.

2.1.2.2.3.3. Görev Değişikliği veya İşten Ayrılma

Kurum personelinin işten ayrılması veya görev değişikliği durumlarında veya üçüncü kişilerle yapılan anlaşmanın sona ermesi halinde bu tarafların kurumun BT varlıklarına erişim haklarını kaldırma, gerektirdiği şekilde yeniden düzenleme, BT varlığının iadesi gibi kuralları içeren yazılı prosedürler olmalıdır.

2.1.2.2.4. Fiziksel ve Çevresel Güvenlik

2.1.2.2.4.1. Güvenli Alanlar

Kurumlar için BT varlıkları, faaliyetlerinin korunması veya devamının sağlanması açısından büyük önem taşımaktadır. Güvenliğin yetersiz olması durumunda işletmenin faaliyetleri tamamen durabilir, ortaya büyük hasarlar veren kesintiler çıkabilir ya da varlıkların ve ticari sırların kaybedilmesi söz konusu olabilir[133]. İşte güvenlik kontrolleri söz konusu bu risklerin açığa çıkmasına karşı alınmış önlemleri ve bu önlemlerin uygulanış biçimlerini ifade etmektedir.

BT varlıklarını ve özellikle bilgi işlem servisini korumak amacıyla bir fiziksel sınır güvenliğinin tesis edilmesi bilgi sistemleri güvenlik planlarının en önemli parçalarından biridir. Yapılan araştırmalar özellikle bilgisayar aracılığıyla gerçekleştirilen yolsuzluklara karşı en etkili önlemin fiziki güvenlik süreçlerinin kuvvetlendirilmesi olduğunu ortaya koymaktadır[134].

Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmalıdır. Hassas bilgilerin bulunduğu alanlar kimlik doğrulama kartı ve PIN koruması gibi yöntemlerle yetkisiz erişime kapatılmalıdır. Örneğin sistem odasına giriş çıkışların manyetik kartlarla kontrol edilmesi ve bu kayıtların loglanması yoluna gidilebilir. Sadece personelin değil, kuruma gelip giden müşteriler ziyaretçiler, tedarikçiler gibi üçüncü kişilerinde giriş çıkış kayıtları kaydedilmelidir. Tüm

---

[133] Hossein Bidgoli ve Reza Azarmsa, Computer Security, "New Management Concern For The 1980s And Beyond", **Journal of Systems Management**, (October 1989), s.21'den Tamer Saka, **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi**, TBB, İstanbul, 2001, s.128.

[134] G.Jack Bologna, Robert J.Lindquist ve Joseph T.Well, **"The Accountant's Handbook of Fraud and Commercial Crime"**, John Willey&Sons, 1993, s.190'dan Tamer Saka, **"Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi"**, TBB, İstanbul, 2001, s.131.

personel ve ziyaretçiler güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartlarını devamlı surette takmalıdırlar. Güvenli alanlara erişim hakları düzenli olarak gözden geçirilmelidir.

BT kritik tesisleri kolayca ulaşılamayacak yerlere kurulmalıdır. Binada bilgi işlem faaliyetlerinin yürütüldüğüne dair işaret, tabela vb. bulunmamasına dikkat edilmelidir. Bilgi işlem merkezlerinin konumunu içeren dâhili/harici telefon rehberleri ortada dolaşmamalı üçüncü kişilere açık olmamalıdır.

Yangın, sel, deprem, patlama ve diğer doğal afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmış olmalı ve uygulanmalıdır. Kurumun komşu olduğu tesislerden kaynaklanan potansiyel tehditleri tespit edilmeli ve risk değerlendirmesinde dikkate alınmalıdır. Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir yerde konuşlandırılmalıdır.

Kayıt yapan cihazların güvenli alanlara sokulmasına engel olunmalıdır. Kullanılmayan güvenli alanlar kilitlenmeli ve düzenli olarak kontrol edilmelidir.

Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir. Bilgi işlem servisleri ile dağıtım ve yükleme alanları ve yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmelidir.

2.1.2.2.4.2. Ekipman Güvenliği

Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine özen gösterilir. Kritik veri içeren ekipmanın yetkisiz kişiler tarafından gözlenemeyecek şekilde konumlandırılmasına önem gösterilmelidir. Kritik BT varlıkları diğerlerinden izole edilmeli ve ortamın nem, sıcaklık gibi parametreleri sürekli izlenmelidir.

BT risk yönetiminde hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, yıldırım çarpması, sel gibi potansiyel tehditlerden kaynaklanan riskler belirlenmeli ve bu riskleri düşürücü kontroller tespit edilip uygulanmalıdır.

Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde olmalıdır. Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmalıdır. Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır. Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

Güç ve iletişim kablolarının fiziksel etkilere ve dinleme faaliyetlerine karşı korunması için önlemler alınmalıdır. Kablolar yeraltında olmalı ve iletişim hatları ile güç kablolarının karışmaması için etiketleme, işaretleme yapılmalıdır. Hassas ve kritik bilgiler için ekstra güvenlik önlemleri alınmalı, alternatif yol ve iletişim kanalları açmalıdır.

Ekipmanın bakımının üreticinin tavsiye ettiği zaman aralıklarında ve tavsiye edilen şekilde sadece yetkili personel tarafından yapılması ve bunların yetkisiz olarak kurum dışına çıkarılmaması hususu denetlenmeli ve tüm kurum çalışanları bu tip denetlemelerden haberdar olmalıdırlar.

2.1.2.2.5. Haberleşme ve İşletim Yönetimi

2.1.2.2.5.1. İşletim Prosedürleri ve Sorumluluklar

Kurumda sistem açma/kapama, yedekleme, cihazların bakımı, bilgisayar odasının kullanılması gibi sistem faaliyetlerine ilişkin prosedürler yazılı olarak mevcut olmalı ve güncellenmelidir. Bu prosedürlere kurumda ihtiyacı olan kullanıcıların erişimi sağlanmalıdır.

2.1.2.2.5.2. Değişim yönetimi

Değişim yönetimi bilgi teknolojilerinde büyük önem taşımaktadır. Sistemler ve uygulama yazılımları etkin bir değişim kontrolüne tabi olmalıdır. Değişiklikler belli bir prosedür çerçevesinde resmi onay mekanizması altında planlanmalı, test edilmeli, etkileri değerlendirilmeli ve daha sonra gerçekleştirilmelidir. Değişikliklerin log kayıtları tutulmalı, başarısız değişikliklerin düzeltilmesi, geri alınması ile ilgili sorumluluklar değişim yönetimi prosedüründe belirlenmelidir. Geliştirme ve test ortamları esas çalışma ortamından ayrı olmalıdır. Örneğin, geliştirilmekte olan yazılım ile kullanılmakta olan yazılım farklı bilgisayarlarda çalıştırılmalıdır.

Bilginin veya bilgi servislerinin sehven ya da kasten yanlış kullanımını veya yetkisiz değiştirilme riskini azaltmak için görevler ve sorumluluklar ayrılmış olmalıdır. Bir işin yetkilendirilmesi ile o işin gerçekleştirilmesi farklı kişiler tarafından yapılmalıdır.

2.1.2.2.5.3. Üçüncü taraflardan alınan hizmetin yönetilmesi

Kurumun tedarikçiler, destek hizmeti sağlayıcıları gibi üçüncü taraftan hizmet almaları durumunda dikkat etmeleri gereken hususlar bulunmaktadır. Bu taraflarla yapılan bakım, destek ve hizmet anlaşmalarında hizmetlerin tanımı, güvenlik seviyeleri açıkça belirtilmeli, alınan hizmetler, raporlar ve kayıtlar düzenli olarak gözden geçirilmeli ve denetlenmelidir.

2.1.2.2.5.4. Sistem Planlama ve Kabul Etme

Sistem performanslarını üst düzeyde tutmak için sistem kaynaklarının kullanım oranları izlenmeli ve ileriye dönük kapasite ihtiyacı projeksiyonları yapılmalıdır. Örneğin kritik sunucular üzerindeki boş sabit disk alanları, hafıza ve işlemci kullanım kapasiteleri izlenmelidir.

Kurumun yürütmekte olduğu faaliyetler ve stratejik planında yer alan yapmayı planladığı faaliyetleri için kapasite ihtiyaçları bunların tedarik süresi, fiyatı gibi kriterler göz önüne alınarak belirlenmelidir.

Yeni sistemin kuruma resmi kabulünden önce bu sistemin mevcut sistemlerle birlikte sorunsuz çalışabilirliği, toplam sistem güvenliğine etkileri, kullanım kolaylığı, eğitim ihtiyacı ve sistemle ilgili diğer konular belirlenmeli ve test edilmelidir.

2.1.2.2.5.5. Kötü Niyetli ve Mobil Yazılımlara Karşı Korunma

Kurumun tüm personeline, yabancı ağlardan ve diğer medyadan dosya ve yazılım alınmasının riskleri, bunlardan korunmanın yolları anlatılmalıdır. Kötü niyetli yazılımlara karşı eğitimler verilerek kullanıcı bilinci oluşturulmalı ve bunların önlenmesi, tespit edilmesi, düzeltilmesi yönünde tedbirler alınmalı, saldırıların rapor edilmesi ve saldırı sonrası tedavi ile ilgili yönetim prosedürleri ve sorumluluklar belirlenmelidir.

Kurumun güvenlik politikası yetkisiz yazılım kullanmayı yasaklamalıdır. Kritik iş süreçlerini çalıştıran sistemler düzenli olarak taranarak yetkilendirilmemiş yazılım ilaveleri veya dosyaların mevcudiyeti bunları bulma ve önleme fonksiyonlarını yerine getiren programlar vasıtasıyla sorgulanmalıdır. Ağ üstünden veya diğer ara yüzlerden masaüstü bilgisayarlara veya sunuculara giren dosyalar, e-posta ekleri ve bağlanılan internet sayfalarının içerikleri kontrol edilmeli ve gerekenler filtrelenmelidir.

Mobil yazılım, bir bilgisayardan diğerine taşınan ve otomatik olarak çalışan yazılımlardır. Bu tür yazılımlardan sadece yetkilendirilmiş olanların kullanımına izin verilmeli, güvenlik politikası uyarınca çalışması konfigürasyon aracılığı ile güvence altına alınmalıdır.

2.1.2.2.5.6. Yedekleme

Yedekleme, temel faaliyetlerin kesintiye uğramadan devamını sağlayan bir süreçtir. Yedekleme kapsamında donanım yedeklemesi, program ve yazılım yedeklemesi ve veri dosyalarının yedeklemesi yapılmalıdır. Etkin bir devamlılık planlamasının önemli adımlarından bir tanesi de donanım yedeklemesidir. Özellikle bankalarda hayati öneme sahip bilgisayar sistemlerinin herhangi bir olumsuzluk karşısında kullanılamaz hale gelmesi durumunda, faaliyetlerin asgari şartlarda yürütülebilmesine imkan verecek donanımın sağlanması için gerekli yedekleme planlarının hazırlanması zorunludur[135]. Program ve yazılım yedeklemesi donanım yedeklemesinin ayrılmaz bir parçasıdır. Çünkü donanım yedeklerinin yazılım desteği olmaksızın kullanılabilmesi mümkün değildir. Program yedeklemesi; işletim sistemi yazılımları, uygulama yazılımları ve yazılı belgeler olmak üzere üç temel alandan oluşmaktadır[136]. Kurumun veri dosyaları hem kurum içinde hem de kurum dışında yedeklenmelidir. Dosyaların en son biçimleri mutlaka günlük olarak, hatta hayati öneme sahip olanlar için saatlik veya anlık yedeklenmelidir[137].

---

[135] FFIEC- Fedaral Financial Institutions Examination Council, **Information Systems Examination Handbook**,1996, s.10'den Tamer Saka, **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi**, TBB, İstanbul, 2001, s.157.
[136] Tamer Saka,**Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi**, TBB, İstanbul, 2001, s.158.
[137] Gordon B. Davis, Donald L Adams ve Carol A. Achaller, **Auditing&EDP**, AICRA, 1983, s.127-128'den Tamer Saka, , s.160.

Öncelikle kurumun bir yedekleme politikası olmalıdır. Bu politika uyarınca yedeklemenin hangi düzeyde, hangi sıklıkta yapılacağı tanımlanmalı, yedeklemenin düzenli olarak yapıldığı, yedeklerin test edildiği kontrol edilmelidir. Bir felaket veya sistem hatasından sonra gerekli tüm bilgilerin ve yazılımların kurtarılmasını sağlayacak yedekleme kabiliyetinin mevcudiyeti sorgulanmalıdır. Program, yazılım ve veri dosyalarının yedeklenmesinde yedeklerin bir kopyası ana sitede meydana gelebilecek bir felaketten etkilenmeyecek mesafede fiziksel ve çevresel etkenlerden korunarak saklanırken bir kopyası da ana merkezden farklı bir bölgede yanmaz kasalarda saklanmalıdır. Kritik öneme haiz veriler şifrelenerek yedeklenmelidir. Yedekleme ortamı düzenli olarak test edilmeli, ömrünü tamamlayan yedekler güvenli biçimde imha edilmelidir. Yedeklerden geri dönüş durumunda işletim prosedürlerinde belirtilen zaman dilimlerine uyum konusu kontrol ve test edilmelidir.

2.1.2.2.5.7. Ağ Güvenliği Yönetimi

Birden fazla bilgisayarın birbirlerine doğrudan ve/veya telefon hatları ile bağlanmasıyla oluşan sisteme bilgisayar ağı (network) denir. Varolma amacı bilgisayar kaynaklarının etkin ve verimli şekilde paylaşımını ve verilere zamanında erişimi sağlamaktır. Bilgisayar ağları fiziksel olarak aynı mekanda bulunan bilgisayarların birbirine bağlanmasıyla oluşan yerel alan ağları (LAN: Local Area Network) ve şehir içi, şehirlerarası, ülkeler arası bilgisayar bağlantıları ile oluşan, örneğin internet gibi geniş alan ağları (WAN: Wide Area Network) olmak üzere ikiye ayrılırlar[138].

Bilgisayar ağlarının maruz kalabileceği riskler genel olarak; gizli bilgilere yetkisiz erişim, veriler üzerinde yetkisiz değişikliklerin yapılması, faaliyetlerin kesintiye uğraması ve verilerin hatalı iletilmesi şeklinde sıralanabilir.

Bu riskleri önlemek için, ağ sistemlerinin unsurlarına ve iletişim araçlarına erişimi engelleyen fiziki ve mantıksal ağ güvenliği kurulmalı, telefon numaraları gizli tutulmalı, tüm erişim noktalarında ton bastırma aygıtlarının kullanımı, ağ sistemine erişim belirli

[138] Saka, s.127.

kullanıcılar ve belirli donanımlarla sınırlanmalı ve başarısız erişim denemeleri kontrol altına alınmalıdır[139].

Ağ yöneticileri, ağlardaki verinin güvenliği ve bağlı bulunan servislere yetkisiz erişimi engellemek için gerekli tedbirleri almalıdırlar. Ağların işletme sorumluluğu mümkün olan yerlerde bilgisayar işletmenlerinden ayrılmalıdır. Uzaktan erişim donanımlarının yönetimi için sorumluluklar ve prosedürler belirlenmelidir. Halka açık ağlardan ve telsiz ağlardan geçen verinin bütünlüğünü ve gizliliği korumak, ağa bağlı sistemleri ve uygulamaları korumak için özel tedbirler alınmalıdır (VPN, erişim kontrolü ve şifrelemeli önlemler gibi). Ağ servislerini optimize etmek ve bilgi işlem altyapısı ile ilgili kontrollerin koordinasyonunu ve kuruluşun tamamında uygulanmasını sağlamak üzere yönetim faaliyetleri gerçekleştirilmelidir. Kurumun içinden sağlanacak veya dışarıdan alınacak ağ hizmetlerinin her birinin yönetilmesi ve güvenliği ile ilgili ihtiyaçlar belirlenmeli, bu ihtiyaçlar hizmet sağlayıcıları ile yapılan anlaşmalarda yer almalıdır.

2.1.2.2.5.8. Bilgi ortamı yönetimi

Kurumda bilginin varolduğu tüm ortamlar bilgi ortamları olarak adlandırılabilir. Bilgi ortamları banka gibi teknoloji yoğun hizmet işletmeleri için son derece değerli varlıklardır. Bu nedenle yazılım ve bilgilerin herhangi bir nedenle zarar görmesi finansal nitelikteki kayıplara neden olabilmektedir. Bilgi ortamlarındaki bilginin güvenliği de bu açıdan büyük önem taşımaktadır[140].

Teyp, disk, disket, kaset, hafıza kartları ve yazılı raporlar gibi sökülebilir bilgisayar ortamlarının yönetilmesi ile ilgili prosedürler olmalıdır. İçinde bilgi ihtiva eden ve daha fazla gerekmediği için kurum dışına çıkarılacak yeniden kullanılabilir ortamlar (disket vs.) bu işlemden önce resmi kayıt altına alınıp, yetkilendirilen kişilerce emniyetli bir biçimde okunamaz hale getirilmelidir. Emniyetli imha işi dışarıdan bir firmaya yaptırılıyorsa gereken güvenlik önlemlerini uygulayan bir firmanın seçilmesine dikkat edilmeli ve imha edilen ortamların kaydı tutulmalıdır.

---

[139] Michael A. Murphy ve Xenia Ley Parker, **Handbook of EDP Auditing, 1994 Cumulative Supplement**, Coopers&Lybrand 1994, s.37-38'den Tamer Saka, s.128.
[140] "Guidelines for the Security of Information Systems", http://www.oecd.org 1992, s.11'den Tamer Saka, s.138.

Taşınabilir hafıza ortamlarını destekleyen ara yüzler gerçekten gerekmedikçe kapalı tutulmalıdır. Tüm ortamlar gizlilik dereceleri uyarınca etiketlenmeli ve yönetilmelidir. Yetkisiz kişilerin bilgiye erişimine engel olmak için erişim kısıtlaması uygulanmalıdır. Bilgiye erişim yetkisi olan kişiler resmi ve güncellenmekte olan bir belgede belirtilmelidir. Veri girdisinin eksiksiz olduğu, işlemin hatasız tamamlandığı ve çıktı onayından geçtiği kontrol edilmelidir. Veri dağıtımının en alt düzeyde tutulması sağlanmalıdır. İşlemler, prosedürler, veri yapıları, yetkilendirme işlemlerinin uygulama tanımları gibi bir dizi duyarlı bilgiyi içeren sistem dokümantasyonu yetkisiz erişimden korunmalıdır. Sistem dokümantasyonu güvenli bir ortamda bulundurulmalıdır. İşlemler, prosedürler, veri yapıları, yetkilendirme işlemlerinin uygulama tanımları gibi bir dizi duyarlı bilgiyi içeren sistem dokümantasyonu yetkisiz erişimden korunmalıdır. Sistem dokümantasyonu güvenli bir ortamda bulundurulmalı, buna erişim listesi asgari düzeyde tutulmalı ve yetkilendirme sistemin sahibi tarafından yapılmalıdır.

2.1.2.2.5.9. Bilgi Değişimi

Her türlü iletişim ortamında bilginin güvenliğini sağlamak için resmi bir değiş tokuş politikası veya prosedürü uygulanmalıdır.

Elektronik iletişim araçları ile ilgili prosedür ve kontroller aşağıdaki durumları düzenlemelidir;

Bilginin kopyalanması, tahribi, içeriğinin veya yolunun değiştirilmesinden korunma. Elektronik iletişim aracılığı ile alınabilecek kötü niyetli yazılımların tespiti ve bertaraf edilmesi. Mesajlara eklenmiş hassas bilgilerin korunması. Elektronik iletişim yöntemlerinin kullanımı ile ilgili rehber ve politikalar. Telsiz veri iletişiminin içerdiği riskler de göz önüne alınarak kullanılması. Bilginin bütünlüğünü ve gizliliğini korumak için şifreleme tekniklerin kullanılması. İş ile ilgili yazışmaların saklanması ve imhası.Fotokopi makinesi, yazıcı ve faks cihazlarında hassas bilgi içeren belgelerin bırakılmaması. Elektronik mesajların harici posta kutularına iletilmemesi için yapılacak düzenlemeler. Personelin telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranması. Cevap verme makinelerine hassas bilgi içeren mesajlar bırakılmaması. Faks cihazlarının kullanılması ile ilgili risklerin personele anlatılması.

Kurum ile diğer taraf arasında bilgi ve yazılım değişiminin şartlarını düzenleyen içerisinde bilgilerinin duyarlılığı ile ilgili güvenlik konularını barındıran anlaşma olmalıdır.

Nakil halindeki bilgi; yetkisiz erişimden, fiziksel zararlardan, bilinçsiz kötü kullanımdan veya yetkisiz değiştirilmelerden korunmalıdır. Bilgi naklinde güvenilir araç veya kuryeler kullanılmalı, kuryelerin kimliği belli bir prosedür çerçevesinde kontrol edilmelidir.

Elektronik olarak taşınan bilgi için de gerekli önlemleri almak gerekmektedir. Mesajlar yetkisiz erişimden korunmalı, mesajın doğru adrese gitmesi sağlanmalıdır. Elektronik posta hizmetinin sürekliliği ve güvenilirliği yüksek olmalı, elektronik imza uygulaması yasal bir yükümlülük olarak benimsenmelidir. Halka açık sistemler kullanılmadan önce yönetimden onay alınmalıdır.

Elektronik ofis sistemlerinin birbirine bağlanması ile ilgili olarak burada bulunan bilginin korunması için politika ve prosedürler geliştirilmeli ve kullanılmalıdır. Kurumdaki operasyonel işlemlerdeki veri için sistemdeki açıklar dikkate alınmalı, bilgi paylaşımının yönetilmesi için politika ve tedbirler olmalıdır.

2.1.2.2.5.10. Elektronik Ticaret Hizmetleri

İnternet aracılığıyla halka açık olan kurumun ticari bilgilerinin hileli kazanç faaliyetleri, anlaşma itilafları, ağ üzerindeki değiştirilme riski gibi bir dizi ağ şebekesi tehdidine karşı korunmuş olması gereklidir. Elektronik ticarete ilişkin bilginin ağ üzerinde maruz kalacağı risklerin çoğu bilginin kriptolanması ile önlenmektedir.

Ticaret ortakları arasındaki elektronik ticaret düzenlemeleri, iki tarafı bilgilendiren, yetkilendirme detaylarının dâhil olduğu, üzerinde anlaşma sağlanan ticari şartların yazılı olduğu bir belge ile tespit edilmelidir.

Çevrimiçi işlemlerle ilgili bilgi hatalı gönderme, hatalı yönlendirme, mesajın yetkisiz kişiler tarafından ifşa edilmesi, değiştirilmesi, kopyalanması veya tekrar gönderilmesine karşı korunmalıdır. Kurumun sistemleri açıklık ve sızma riskleri için test edilmelidir.

2.1.2.2.5.11. İzleme

Erişimi izlemek ve gerektiğinde soruşturmalarda kullanmak üzere gerekli sistemlerde kullanıcı faaliyetleri ve güvenlik ile ilgili olay kayıtları tutulmalı ve bunlar belirli bir süre saklanmalıdır. Kullanıcı kimlikleri, kullanıcıların oturuma giriş ve çıkış tarihleri ve zamanları, terminal kimlikleri, başarılı ve reddedilmiş sistem erişim denemeleri, sistem konfigürasyonunda yapılan değişiklikler, erişilen dosyalar ve programlar ile ilgili kayıtlar loglanmalıdır.

Sistem yöneticilerinin kendi yaptıkları işlemler loglanmalı ve bu logları sistem yöneticileri dahi silememelidir. Bilgi işlem araçlarının kullanımının izlenmesi ile ilgili prosedürler geliştirilmeli ve uygulanmalıdır.

Sistem kullanım kayıtları düzenli olarak gözden geçirilmelidir. Risk değerlendirme çalışması sonucunda, bilgi işlem araçlarında yapılan işlemlerin hangi düzeyde kaydedileceği belirlenmelidir. Kayıt alma araçları ve kayıt bilgileri yetkisiz erişim ve değiştirmeye karşı korunmalıdır.

Başarılı veya başarısız faaliyetin tarihi ve zamanı, faaliyetle ilgili bilgi, işlemin hangi kullanıcı hesabı üstünde ve hangi yönetici tarafından yapıldığı, hangi süreçlerin etkilendiği kaydedilmeli ve işletmen kayıtları düzenli olarak incelenmelidir.

Bilgi işlem ya da iletişim sistemleri ile ilgili olarak kullanıcılar tarafından rapor edilen hataların kaydı tutulmalıdır. Hataların tatmin edici bir şekilde giderildiğinden emin olmak için hata kayıtları gözden geçirilmelidir.

Sistem bilgisayarları veya diğer bilgi sistemi cihazlarının saatleri standart bir zaman bilgisine göre ayarlanmalıdır. Bilgisayar saatlerinin doğru ayarlanmış olması farklı bilgisayarlardan alınmış olay kayıtlarının birlikte incelenebilmesi açısından büyük önem arz etmektedir.

2.1.2.2.6. Erişim Kontrolü

2.1.2.2.6.1. Erişim Kontrolü için İş Gereksinimleri

Erişimle ilgili iş ve güvenlik ihtiyaçları göz önünde bulundurularak erişim denetimi politikası oluşturulmalı ve belgelenmelidir. Erişim denetimi hem fiziksel, hem işlevsel boyutları ile değerlendirilmelidir. Erişim denetimi politikası bütün kullanıcılar veya kullanıcı grupları için erişim kurallarını ve haklarını belirtmelidir. Kullanıcılara ve servis sağlayıcılarına erişim denetimiyle hangi iş gereksinimlerinin karşılanacağı açıklanmalıdır. Erişim haklarının "yasaklanmadıkça her şey serbesttir" değil "izin verilmedikçe her şey yasaktır" prensibine göre verilmesine dikkat edilmelidir.

Politika belgesi her bir iş sürecinin güvenlik ihtiyaçlarını, iş süreçleri ile ilgili tüm bilgiler ve bu bilgilerin yüz yüze olduğu riskleri, bilginin yayılması ve yetkilendirme ile ilgili politikaları, bilginin sınıflandırılması ve güvenlik seviyelerini, farklı sistem ve ağlardaki bilginin sınıflandırılmasını, kurumun yaygın kullanıcı profilleri ile ilgili erişim hakları ve erişimin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması hususlarını içermelidir.

2.1.2.2.6.2. Kullanıcı Erişiminin Yönetilmesi

Bilgi sistemlerine ve servislerine erişim hakkı vermek için resmi bir kullanıcı kaydı girme ve kullanıcı kaydı silme prosedürü olmalıdır.

Kullanıcı kimlik tanımlaması sisteme erişimin birinci aşamasını sağlarken, şifre kullanıcının sisteme erişim için yetkisini ortaya koyar, tasdik eder. Kullanıcı kimlik tanımlanması hangi kullanıcının sisteme girdiğinin belirlenmesinde kullanılmaktadır. Ayrıca bu kullanıcı tarafından yürütülen işlemlerin izlenebilmesi için denetim izi görevi de görmektedir. Bu nedenle sistem kayıtları ile ilişkilendirme ve sorumlu tutulabilme açısından kullanıcı kimliklerinin her kullanıcı için farklı olmasına dikkat edilmelidir[141]. Bir kullanıcıya, kullanıcı tanımlamaları ve şifreleri verilmeden önce, bağlı olduğu birimin yöneticisi tarafından söz konusu kullanıcı için güvenlik erişim seviyesi tanımlanmış ve uygulama için güvenlik yöneticisine iletilmiş olmalıdır. Erişim seviyeleri ve kuralları kullanıcıların mevcut

[141] Thomas Negron, "Audit Concerns in the PC Environment", Internal Auditing, Winter 1992, s.38-43'den Tamer Saka, s.141.

pozisyonlarına, kurumsal güvenlik politikasına ve görevler ayrılığı ilkesine uygun olarak belirlenmelidir[142].

Kullanıcılara erişim haklarını anlatan bir prosedürle açıklanmalı ve kullanıcılardan erişim şartlarını anladıklarına ilişkin imzalı belge alınmalıdır. Görevi değişen veya kuruluştan ayrılan personelin erişim hakları derhal güncellenmelidir.

Kullanıcı parolalarının atanması ya da değiştirilmesi resmi bir prosedür uyarınca yapılmalıdır. Kullanıcılara parolalarını saklı tutacaklarına dair bir taahhütname imzalatılmalıdır. Kullanıcı erişim haklarının düzenli aralıklarla kontrol edilmesini sağlayan resmi bir süreç olmalıdır.

2.1.2.2.6.3. Kullanıcı Sorumlulukları

Erişim güvenliğinin sağlanmasında kullanıcıların sisteme bağlanmasını sağlayan parolaların belirlenmesi ve yönetilmesi için geliştirilen standartlar büyük önem taşımaktadır. Şifreler ağ sistemine karşı gerçekleştirilen saldırılarda kullanılan ilk savunma hattıdır. Şifrelerin kullanımı ile ilgili olarak etkinliklerini arttırmak amacı ile bazı sınırlamalar ve standartlar bir prosedürle yazılı hale getirilmelidir.

Kullanıcılara şifreleri belirleme konusunda yetki verilen durumlarda, kullanıcı tarafından seçilecek şifrelerin karakter uzunluğunun en az ne olacağı önceden belirlenmiş olmalıdır. Şifrelerin kolay tahmin edilecek kombinasyonlardan oluşturulmaması konusunda kullanıcılar bilinçlendirilmelidir. Örneğin şifrelerin hem sayısal hem de sayısal olmayan karakterlerden oluşturulması hususu sistem tarafından kontrol edilip bu standarda uymayan şifrelerin tanımlanması önlenebilir.

Belli aralıklarla şifrelerin değiştirilmesi şifre güvenliğinin önemli bir parçasıdır. Bununla beraber değişim sıklığı da dikkatle ayarlanmalıdır. Sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesi sağlanmalıdır. Şifrelere kullanıcı zaman ve konum kontrolleri getirilebilir. Bu kontrollerin amacı, veri iletimi veya diğer işlemlerin yürütülmesini belirli zaman aralıkları ve belirli donanımların kullanımı

[142] Murphy ve Diğerleri, s.31'den Tamer Saka, s.141.

ile sınırlandırmaktır. İşlem kayıtları ağ güvenliğinin önemli unsurlarından biridir. Sisteme girişi için yapılan her deneme ister başarılı olsun ister başarısız mutlaka loglanmalıdır.

Kişisel parolaların hiç kimse ile paylaşılmamasına, yazılı veya elektronik ortamlarda kaydedilmemesine dikkat edilmeli, kullanıcılar düzenli aralıklarla veya sistem güvenliği ile ilgili bir kuşku oluştuktan sonra parolalarını değiştirmeye zorlanmalıdır. Kullanıcılar kişisel işlerinde kullandıkları parolaları kurumun iş süreçlerinde kullanmamaları gerektiği konusunda bilinçlendirilmelidir.

Kurumda tüm çalışanların temiz masa, temiz ekran politikasından haberdar olması bilgi güvenliğinin sağlanmasının önemi koşullarından biridir. Bu politika ile kullanıcılar ve iş ortakları atıl cihazlara ait güvenlik gereksinimlerinden, bu cihazları koruma prosedürlerinden ve bu cihazları korumak için üzerlerine düşen sorumluluklardan haberdar olurlar. Örneğin kullanıcıların bilgisayarlarını geçici süre ile terk ettiklerinde oturumunu kapaması veya ancak parola ile açılabilen ekran koruyucu vb. önlemleri devreye sokması veya hassas bilgileri içeren kâğıt ve elektronik depolama ortamlarının, bilgi ve belgelerin mesai bitiminde ortalıkta bırakılmaması, mümkünse kilitli ortamlarda kullanılmadığı zaman saklanması, bilgisayar, gelen/giden postaya erişim noktalarının ve faks cihazlarının denetlenmesi, fotokopi makinesi, tarayıcı, sayısal fotoğraf makinesi gibi kopyalama teknolojilerinin yetkisiz olarak kullanılmaması, hassas bilgi içeren dokümanların yazıcı üstünde bırakılmaması konularına özen gösterilmelidir.

2.1.2.2.6.4. Ağ Erişim Kontrolü

Kullanıcıların sadece kullanma yetkisine sahip oldukları ağ servislerine erişebilmesi sağlanmalıdır. Kurumun ağlar (network) ve ağ servisleri ile ilgili olarak bir politikası olmalıdır. Bu politika ile kimin hangi ağlara ve ağ servislerine erişebileceğini belirleyen bir yetkilendirme prosedürü tanımlanmalıdır. Ağ bağlantılarını korumak ve ağ servislerine erişimi engellemek için süreçler belirlenmeli ve denetlenmelidir. Sisteme dışarıdan yapılacak kullanıcı bağlantıları için kullanıcı kimliği doğrulama mekanizmaları uygulanmalıdır. Bağlantının belli bir cihaz kullanılarak yapıldığından emin olmak için otomatik cihaz kimliği belirleme yöntemleri kullanılmalıdır. Kablosuz ağlar dışarıdan sızmalara daha açık olduklarından bunlarla ilgili önlemler alınmalıdır.

Kurum sınırlarının dışına taşan ağlar ve ağ bağlantılarının kullanımı kurumun erişim kontrol politikası uyarınca kısıtlanmalıdır. Elektronik mesaj, tek veya çift yönlü dosya aktarımı, interaktif erişim, bağlantı zamanı ve süresi ile ilgili kısıtlamalar olmalıdır. Ağ yönlendirme kontrolleri, bilgisayar bağlantılarının ve bilgi akışının erişim politikasına uygun gerçekleşmesini sağlayacak şekilde tanımlanmış olmalıdır. Ağ iletişimi kaynak adres ve hedef adreslere bağlı olarak güvenlik duvarı vb. cihazlar aracılığı ile kontrol edilmelidir.

2.1.2.2.6.5. İşletim Sistemi Erişim Kontrolü

Oturum açma işlemleri yetkisiz erişim olasılığını asgari düzeye indirecek şekilde düzenlenmelidir. Sistem ve uygulamaya ilişkin olarak yetkisiz kullanıcıya yardımcı olabilecek bilgiler oturuma giriş başarıyla tamamlanana kadar gizlenmelidir. Bilgisayarda sadece yetkili personel tarafından erişilebileceğini bildiren uyarı mesajı gösterilmelidir. Oturuma giriş sadece tüm girdi verilerinin doğrulanmasından sonra sağlanmalıdır. Bir hata durumu varsa sistem verinin hangi kısmının doğru veya yanlış olduğu bilgisini gizlemelidir. Sistem tarafından izin verilen başarısız giriş denemelerine sınırlama getirilmelidir. Oturuma giriş işlemi için bir zaman sınırı olmalıdır. Başarısız giriş denemeleri kaydedilmeli belli bir sayıda sistem kilitlenmelidir. Ağ üstünden şifrenin açık olarak gönderilmemesi sağlanmalıdır.

2.1.2.2.6.6. Uygulama ve Bilgi Erişim Kontrolü

Erişim kontrolü politikası uyarınca kullanıcılar ve destek personeli için bilgi sistemleri fonksiyonları ve bilgilerine erişim kısıtlanmalıdır. Kullanıcıların bilgiyi yazma, okuma, silme veya çalıştırma hakları düzenlenmelidir. Uygulamanın duyarlılığı uygulama sahibi tarafından açıklanmalı ve belgelenmelidir. Hassas ve kritik bilgilerin bulunduğu sistemler diğer sistemlerden fiziksel veya işlevsel olarak izole edilmelidir.

2.1.2.2.6.7. Mobil Bilgi İşleme ve Uzaktan Çalışma

Kurumun taşınabilir araçların kullanımına yönelik bir politikası olmalıdır. Bu politika ile dizüstü bilgisayar, cep bilgisayarı, cep telefonu, akıllı kartlar gibi bilgi işlem ve iletişim araçlarının yetkisiz kullanılmasından kaynaklanan risklerden korunmak için

güvenlik önlemleri belirlenmelidir. Politika fiziksel koruma, erişim denetimi, kriptografik denetimler, yedekleme ve virüs koruması konularını içermelidir.

Mobil bilgi işlem araçlarının halka açık yerler, toplantı odaları gibi korumasız ortamlarda kullanılması sırasında yetkisiz erişime, çalınmasına ve bilginin açığa çıkmasına karşı kriptografik tekniklerin kullanılması gibi önlemler alınmalıdır. Uzaktan çalışma faaliyetleri için organizasyonun güvenlik politikasına uygun plan ve prosedürler geliştirilmelidir. Uzaktan çalışmanın yapılacağı yerde ekipman ve bilginin çalınmasına, bilgiye yetkisiz erişim yapılmasına, kuruluşun dahili sistemlerine uzaktan yetkisiz erişime ve bilgi işlem araçlarının kötüye kullanılmasına engel olmak için uygun önlemler alınmalıdır.

2.1.2.2.7. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı

2.1.2.2.7.1. Bilgi Sistemlerinin Güvenlik Gereksinimleri

Yeni sistemlerin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Sistem geliştirilirken işin başından itibaren güvenlik ihtiyaçları göz önünde bulundurulmalıdır. Satın alınan ürünler için resmi bir test ve tedarik süreci işletilmelidir.

2.1.2.2.7.2. Uygulamaların Doğru Çalışması

Kurumun uygulama programlarına doğru ve uygun bilginin girdiği kontrol edilmelidir. Örneğin kurumda birden fazla birimin veya kullanıcının ortak kullanımında olan döviz kurları, vergi oranları gibi parametre tablolarında yapılan işlemlere daha fazla kontrol uygulanmalıdır. Doğru girilmiş bilginin işlem sırasında hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalarda kontrol mekanizmaları oluşturulmalıdır. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır. Saklanan bilgilerin üstünde gerçekleştirilen işlemlerin doğru ve şartlara uygun olduğundan emin olmak için uygulama çıktılarının denetimi yapılmalıdır. Çıktı verilerinin makul değerler alıp almadığı, tüm verinin işlenip işlenmediği, çıktı veriyi işleyen sisteme verinin bütünlüğünü ve doğruluğunu sınamasını sağlayacak bilginin verilip verilmediği kontrol edilmelidir.

2.1.2.2.7.3. Kriptografik Kontroller

Kurum taşınabilir ortamlar ve iletişim kanallarındaki hassas ve kritik bilgilerin korunmasına yönelik kriptografik önlemler ve uygulamaları düzenleyen bir politika geliştirmelidir. Bu politikada; bilginin korunması ile ilgili genel prensipler ve kullanılacak güvenlik seviyesine karar vermek için risk değerlendirmesinin nasıl yapılması gerektiği, kriptografik tekniklerin kullanmasına imkân sağlayacak güvenlik hususlarının anahtar yöntemi ile düzenlenmesi, algılanan risk ve kullanım şartları uyarınca anahtarların sınırlı bir süre boyunca kullanılabilmesi için gereken düzenlemelerin yapılması, anahtarın saklanması, anahtarın kaybolması durumunda şifrelenmiş bilginin nasıl kurtarılacağı, bu konudaki roller ve sorumluluklar yer almalıdır.

2.1.2.2.7.4. Sistem Dosyalarının Güvenliği

Kurumda sistem dosyalarının güvenliği için de bir takım güvenlik önlemleri alınmalı ve politikalar oluşturulmalıdır. Kullanıcıların sisteme herhangi bir yazılım yüklemesi engelleyen prosedürler düzenlenmelidir. Yazılım yükleme, eğitimli sistem yöneticileri tarafından ve sadece yönetim yetkilendirmesi ile yapılmalıdır.

Çalışan sistemde geliştirilmekte olan yazılım ve derleyici bulunmaması sağlanmalıdır. İşletim sistemi ve uygulama yazılımlarının iyice test edilmeden yüklenmemesine dikkat edilmelidir. Konfigürasyon kontrol sistemi aracılığı ile eski ve yeni yazılım sürümleri, yazılımla ilgili dokümantasyon ve konfigürasyon bilgileri ve sistem dokümantasyonu saklanmalıdır. Üçüncü taraflardan alınmış yazılımın kullanılması, güvenliği ve bakımı ile ilgili riskler göz önünde bulundurulmalıdır. Sistem testi için kullanılan veri dikkatle oluşturulmalı ve korunmalıdır. Test verisinde kurumun aktif veri tabanındaki bilgiler kullanılmamalıdır. Şayet kullanılması mutlaka gerekiyorsa içindeki gizli bilgiler çıkartılmalıdır. Program kaynak kodlarının bulunduğu kütüphanelere erişim ciddi şekilde denetlenerek yetkilendirilmemiş, kontrolsüz değişiklikler engellenmelidir.

2.1.2.2.7.5. Geliştirme ve Destek Süreçlerinde Güvenlik

Bilgi sistemleri üzerinde yapılacak değişiklikler resmi kontrol prosedürleri aracılığı ile denetlenmelidir. Yeni sistem ilaveleri ve büyük değişiklikler resmi bir belgeleme, tarif,

test ve kalite kontrol süreci uyarınca gerçekleştirilmelidir. İşletim sisteminde yapılan değişikliklerin ardından kritik uygulamaların gözden geçirilip test edilmesini sağlayan süreç veya prosedürler geliştirilmelidir. Değişiklik gerçekleştirilmeden belli bir zaman önce ilgili yerlere haber verilerek test ve gözden geçirmelerin yapılması sağlanmalıdır.

Lisans anlaşması, fikri mülkiyet hakları, kalite güvencesi, denetleme için erişim hakkı, kurulum öncesi "Trojan" kod araması için test yapılması gibi hususlar dış kaynaklı yazılım geliştirme faaliyetleri kapsamında izlenmeli ve denetlenmelidir.

2.1.2.2.7.6. Teknik Açıklık Yönetimi

Kullanılan bilgi sistemlerinin teknik açıklıkları ile ilgili bilgiler zamanında toplanmalı, bunlara bağlı olarak kurumun nasıl etkileneceği değerlendirilmeli ve riski azaltmak için uygun tedbirler alınmalıdır. Teknik açıklık yönetimi ile ilgili rol ve sorumluluklar belirlenmelidir.

2.1.2.2.8. Bilgi Güvenliği Olayları Yönetimi

2.1.2.2.8.1. Bilgi Güvenliği Olaylarının ve Zafiyetlerin Rapor Edilmesi

Güvenlik olaylarını mümkün olduğunca hızlı bir şekilde raporlamaya yarayan resmi bir raporlama prosedürü olmalıdır. Raporlama prosedürü ve başvuru noktası tüm personel tarafından bilinmelidir. Başvuru noktasındaki personel her zaman ulaşılabilir durumda ve olaya müdahale edebilecek yetkinlikte olmalıdır. Tüm personel ve üçüncü parti çalışanlarına karşılaştıkları bilgi güvenliği olaylarını hızla bildirme konusunda yükümlü oldukları bu prosedürde yer almalıdır.

2.1.2.2.8.2. Bilgi Güvenliği Olaylarının Yönetimi ve İyileştirmeler

Bilgi güvenliği olaylarına hızlı, etkili ve düzenli bir biçimde karşılık verebilmek için yönetime ait sorumluluk belirlenmiş ve prosedüre edilmiş olmalıdır. Bilgi sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilgi sisteminin kötüye kullanılması, denetim sonuçları ve delillerin toplanması ve güvenli bir biçimde saklanması, bilgi sistemlerinin bütünlüğünün

asgari gecikme ile sağlanması hususlarında alınacak aksiyon bu prosedürde açıklanmış olmalıdır.

Bilgi güvenliğinden kaynaklanan kayıp veya olası kayıp olayları kurumun operasyonel risk kayıp veri tabanına kaydedilmelidir. Geçmiş bilgi güvenliği olaylarından sağlanan tecrübe tekrarlanan veya büyük hasar meydana getiren olayların tespit edilmesinde kullanılmalıdır.

2.1.2.2.9. Bilgi Güvenliği Açısından İş Süreklilik Yönetimi

Kurum bünyesinde bilgi güvenliği ihtiyaçlarına cevap veren, iş sürekliliği için geliştirilmiş bir süreç olmalıdır. Bu süreçte; kuruluşun yüz yüze olduğu riskler, kritik iş süreçleri ile ilgili varlıklar, bilgi güvenliği olayları yüzünden gerçekleşebilecek kesintilerin etkisi, ilave önleyici tedbirlerin belirlenmesi ve uygulanması gibi konular yer almalıdır.

İş süreklilik süreci kapsamında kurumda tüm birimlerin katılımıyla bir iş süreklilik planı oluşturulmalıdır. Bu planın ilk aşaması olan iş etki analiz çalışmasında; kurumun kritik faaliyetlerinin neler olduğu, iş süreçlerinde kesinti yaratan veya yaratabilecek olaylar, kesintilerin yaratacağı finansal, operasyonel ve itibar/imaj etkisinin boyutları, gerçekleşme olasılıkları ve bilgi güvenliği açısından sonuçları, kurumun ilgili faaliyet/sistem kesintisine azami dayanma süresi, sisteme geri dönüş zamanı, bunun için gerekli olan kaynakların planlaması gibi konularda analizler yapılır.

Kurumun kritik iş süreçlerinde meydana gelen kesintilerin etkisini belirlemek için yapılacak risk analizi çalışması sadece bilgi işlem değil tüm iş süreçlerini göz önünde bulundurarak ve tüm süreçlerin sahipleri ile birlikte gerçekleştirilmelidir. Risk analizinin sonuçları uyarınca iş sürekliliği ile ilgili geniş kapsamlı strateji belirlenmelidir. Kritik süreçlerin kesintiye uğramasının ardından kurum tarafından belirlenmiş zaman aralığı içinde iş sürecinin onarılması ve belli bir seviyedeki bilgiye ulaşılabilmesi için planlar geliştirilmelidir. Plan, sorumlulukların belirlenmesi ve anlaşılması, kabul edilebilir hasarın belirlenmesi, onarım prosedürünün belirlenmesi, prosedürün düzenli aralıklarla test edilmesi ve belgelenmesi konularını içermelidir. Tüm planların tutarlı olması, bilgi güvenliği ihtiyaçlarının tutarlı olarak sağlanması, test ve bakımla ilgili önceliklerin belirlenmesi için iş sürekliliği planları tek bir çerçeve uyarınca hazırlanmalı ve güncellenmelidir.

İş sürekliliği planı; bilgi sistemleri erişilebilirliği ile ilgili yaklaşımını, kurtarma planı ve planın harekete geçirilmesi için gereken şartları, planın bölümlerini yerine getirmekle sorumlu kişileri, planın sahibini açıkça belirtmelidir. İş sürekliliği planları güncellik ve etkinliklerinin sınanması açısından düzenli olarak test edilmelidir. Testler aracılığı ile onarım ekibinin üyeleri ve diğer ilgili personelin planlardan ve iş sürekliliği ile ilgili sorumluluklarından haberdar olduğu ve plan devreye sokulduğu zaman üstlenecekleri rolün ne olduğunu bilip bilmedikleri sınanmalıdır.

2.1.2.2.10. Uyum

Bu bölümde; yasal gereklere uyumluluk, güvenlik politikası ve standartlar ile uyum, teknik uyum ve bilgi sistemleri denetimi ile ilgili hususlar açıklanacaktır.

2.1.2.2.10.1. Yasal Gereklere Uyumluluk

Kurumun bilgi sistemleri için ilgili bütün yasal, düzenleyici ve sözleşmeye bağlı gereksinimler ve gereksinimleri sağlamak için kullanılacak kurumsal yaklaşım kontroller ve bireysel sorumluluklar açık şekilde tanımlanmalı ve belgelenmelidir.

Kullanılmakta olan yazılım ve diğer her türlü materyal ile ilgili olarak yasal kısıtlamalara uyulması açısından kopya hakkı, düzenleme hakkı, ticari marka gibi hakların kullanılmasını güvence altına alan prosedürler yazılı olmalıdır.

Fikri mülkiyet olabilecek materyalin korunması için kurumun bir “Fikri Mülkiyet Haklarına Uyum” politikasının olması ve bu politikanın; kullanım haklarının çiğnenmemesi için yazılımın sadece güvenilir kaynaklardan sağlanması, mülkiyet haklarını ispatlamak için delil olarak kullanılabilecek lisans sözleşmesi, orijinal disk, kullanıcı rehberi vb. materyalin saklanması, azami kullanıcı sayısının ihlal edilmemesini sağlamak için gerekli tedbirlerin alınması, yazılım ve diğer ürünler için sadece lisanslı versiyonların kullanıldığının kontrollerle denetlenmesi, film, müzik, kitap, makale ve diğer materyalin telif hakkı kanununun izin verdiği şartlar dışına çıkarak format dönüşümüne tabii tutulmaması, kısmen veya tamamen kopyalanmaması ve çoğaltılmaması gibi hususlara ilişkin maddeleri içeriyor olması gerekmektedir.

Organizasyonun önemli kayıtları kanun, kontrat, anlaşma ve işin doğasından kaynaklanan gereksinimler uyarınca kaybolmaya ve bozulmaya karşı korunmalıdır. Kayıtların saklanması için kullanılan ortamın zaman içinde bozulabileceği göz önünde bulundurulmalıdır. Veri saklama sistemi seçilirken belli bir süre sonra teknoloji değişikliği dolayısıyla kayıtların okunamaz hale gelmemesi için gerekli tedbirler alınmış olmalıdır. Donanımsal ve yazılımsal format uyumunu sağlamak için gerekli program ve teçhizat kayıtlarla birlikte saklanmalıdır.

Yasalar veya mevcut kontratlar uyarınca veriyi ve kişisel bilgilerin gizliliğini korumak için kurumsal politika ve kontroller oluşturulmalıdır. Kişisel bilginin işlenmesi ile ilgisi olan tüm personel politikadan haberdar edilmelidir. Kullanıcıların bilgi işlem tesislerini yönetim tarafından yetkilendirilmemiş işler için kullanmasına engel olunmalıdır. Tüm kullanıcılara bilgi işlem tesisinin kullanımı ile ilgili yetkililerin ne olduğu yazılı olarak bildirilmeli ve bu belgeler kullanıcılara imzalatıldıktan sonra kurum tarafından muhafaza altına alınmalıdır. Yetkisiz erişim tespit edildiği takdirde bu durum disiplin sürecinin veya yasal sürecin devreye sokulması için ilgili kullanıcının yöneticisine bildirilmelidir. Oturum açıldığında bilgisayar ekranında “girilen sistemin kuruma ait olduğunu ve yetkisiz girişe izin verilmediğini” belirten uyarı mesajı ile kullanıcılar uyarılmalıdır.

2.1.2.2.10.2. Güvenlik Politikası ve Standartlar ile Uyum

Yöneticiler kendi sorumluluk alanlarında güvenlik politikalarına ve standartlara uyum açısından güvenlik prosedürlerinin doğru olarak uygulanıp uygulanmadığını kontrol etmelidir. Kontrol ya da gözden geçirme sonucunda bir uyumsuzluğun bulunması halinde yönetici uyumsuzluğun nedenini ve tekrar etmemesi için alınması gereken tedbirleri belirlemelidir. Tedbirin uygulanmasını sağlanmalı ve sonuçlarla birlikte kayıt altına alınıp gözden geçirilmelidir.

2.1.2.2.10.3. Teknik Uyum

Bilgi sistemleri, güvenlik uygulama standartları ile uyumun sağlanması için düzenli olarak kontrol edilmelidir. Teknik uyumluluk testleri sadece yetkili personel eşliğinde yapılmalıdır. Sızma (Penetrasyon) testleri ve açıklık analizleri sırasında sistem güvenliğinin sekteye uğramaması için gerekli tedbirler alınmalıdır.

2.1.2.2.10.4. Bilgi Sistemleri Denetimi İle İlgili Hususlar

Kurumun bilgi sistemleri diğer operasyonel birimler gibi düzenli olarak denetlenmelidir. Denetleme gereksinim ve aktiviteleri dolayısıyla çalışmakta olan sistemler üstünde kontroller yapılırken, iş sürecinin asgari düzeyde zarar görmesi için dikkatle planlama yapılmalıdır. Denetim gereksinimleri ve kapsamı konusunda yönetim ile anlaşmaya varılmalıdır. Yazılım ve veri ile ilgili kontroller salt okuma şeklinde gerçekleştirilmelidir. Yazılım ve veri dosyaları gibi sistem denetleme gereçlerine erişim, herhangi bir yanlış veya kötü niyetli kullanıma karşı koruma altında olmalıdır. Sistem denetleme gereçleri ilave koruma sağlanmadıysa geliştirme sisteminden ve çalışmakta olan sistemden ayrılmalıdır.

2.2. İnsan Kaynaklı Operasyonel Riskler ve Yönetimi

Bilgisayar sistemlerinde ve teknolojide görülen hızlı gelişim ve buna bağlı olarak maliyetlerdeki düşüş, bu sistemleri insan faktörüne göre daha avantajlı kılmıştır. Zira "otomasyon", operasyonel risklerin önlenmesinde önemli bir halkadır. Son zamanlarda finansal kuruluşlar tarafından sunulan ürün ve hizmetlerin giderek daha karmaşık hale gelmesi de bu sistemlerin kullanımını vazgeçilmez hale getirmiştir. Bununla birlikte faaliyetlere ilişkin tüm işlemlerin bilgisayarlar ile yapılması mümkün değildir. Bu nedenle, finansal kuruluşların faaliyetlerinde önemli bir unsur olan ve operasyonel risklerin önemli bir kaynağını oluşturan insan faktörünün yönetimi, risklerin önlenmesi açısından hayati bir öneme sahiptir.

İnsan kaynaklı operasyonel risklerin kaynakları; kurumsal organizasyon yapısı, işin niteliği/tanımı ve kişisel etmenler olarak sayılabilir.[143] Kurumlar, çalışanlarının dahil olmasını ve her bir işlem ve faaliyette ona uygun olarak hareket etmesini sağlayacak, belirlenen sınırlar ve normlar dışında hareket edilmesinin kesinlikle kabul edilemeyeceği bir risk yönetim kültürünü organizasyonel yapı içine entegre etmelidir. İşin tanımı ve niteliğinden kaynaklanan riskler ise personelin yetenek, tecrübe ve kapasitesiyle işin nitelikleri arasındaki uyumsuzluktan kaynaklanan hataların sebebiyet verdiği olaylardır. İnsan kaynaklı operasyonel riskler arasındaki kişisel etmenler, personelin kendi

[143] Mestchian'den Moosa, s.216.

özelliklerinden kaynaklanan risk noktaları olarak ortaya çıkabilir. Çünkü, işe alımlar gerçekleşirken çalışanların alışkanlıkları, tecrübeleri, davranış tarzları gibi konularda daha fazla bilgi edinmek için çeşitli kişilik testleri ve mülakatlar gerçekleştiriliyor olsa da her zaman çalışanları en iyi şekilde tanımak mümkün olamayabilir. İnsan faktörünün bazı yetenek ve tecrübe eksikliklerini çeşitli eğitimlerle tamamlayabilmek mümkünken, kişisel karakter gibi özellikleri değiştirmek doğal olarak imkansız yada oldukça zordur.

2.2.1. Öğrenen Organizasyonlar Yaratmak

Ekonomik ve finansal sistemdeki küreselleşme trendlerine paralel olarak iş dünyasında hacimlerin büyümesi, teknolojik imkanların gelişmesi, artan ve çeşitlenen müşteri beklentileri ve rekabet ortamının giderek daha da sertleşmesiyle şirketler farklı risklerle karşılaşmaktadırlar[144]. Artan ve farklılaşan riskler karşısında kurumlar kendilerini savunmak ve bu riskleri yönetmek zorunda hissetmektedirler ve bunun için de risk yönetimi konusunda kurumsal öğrenmeyi gerçekleştirmek gerekmektedir. Kurumsal öğrenmenin içselleştirilmesiyle beraber kurumlar değişimlere ayak uydurabilmekte, önceden gerçekleştirmiş oldukları hatalardan kaçınmakta, sahip oldukları kritik bilgi birikimini kurum içinde tutabilmekte ve rekabet içinde bir adım öne geçebilmektedirler.

Kurumsal öğrenmenin alt yapısının oluşturulmasında, öncelikle söz konusu olan kurumun kendisini öğrenen bir kurum haline dönüştürmesidir. Öğrenen kurum; ürünlerini, hizmetlerini, iş süreçlerini hep yeniden gözden geçiren, iyileştiren, takımlar halinde ve bireysel olarak çalışanlarını risk yönetimi konusunda eğiten ve tecrübe kazandıran bir kurumdur. Bu kapsamda, kurumlar personelin risk yönetimi konusunda inisiyatif ve tecrübelerini geliştirmeleri için çok çeşitli eğitim ve tecrübe kanallarını oluşturmalıdırlar. Risk yönetimine ilişkin olarak gerçekleştirilen eğitim ve tecrübe aktarımlarıyla kurumsal risk yönetimi tecrübesi artmakta, farklı birimlerin maruz kaldığı riskler karşısında geliştirmiş oldukları tecrübeler diğer birimlerin kullanımına aktarılabilmektedir. Kurumlar geleneksel olarak kurum içinde düzenlenen eğitimlerin yanı sıra teknolojinin sunduğu en üst düzeydeki imkanları kullanarak kurumsal portal üzerinden, online eğitim imkanları sağlayarak, etkin yardım masaları kurarak risk yönetimi konusunda personelin tecrübesini ve bilgiye erişimini kolaylaştırmaktadır. Gelişmiş doküman yönetim sistemlerinin kullanımı, hata ve istisnaları

[144] Hussain, s.143.

tespit etmeye dönük yazılımlar da risk yönetimi konusunda kurumsal öğrenmeyi daha etkin hale getirmektedir. Risk yönetimi karşısında elde edilen tecrübeler kurumsal bilgi ağına eklenmeli, ilişkili uygulama talimatları ve prosedürler oluşturulmalıdır[145].

2.2.2. İş ve Görev Tanımları

Kurumda personelin görev, yetki ve sorumluluklarının yazılı olarak belirlenmesi, işe alınırken kendisine tebliğ edilmesi, kolayca ulaşabileceği bir portala, ortama kayıt edilmesi, gerektiğinde güncellenmesi operasyonel risk yönetiminin insan faktörüne ait önemli noktalarını içermektedir.

İş tanımlarını, görevleri ve çalışanların niteliklerini belirleyen ilk unsur kurumun faaliyetlerinin türü ve niteliğidir. Çünkü, gerek hizmet sektöründe olsun gerekse de üretim sektöründe, ürünlerin ve hizmetlerin sunumu, talebin ve ürünün özelliklerine bağlı olarak farklılık gösterebilmektedir. Çünkü, bazı ürünler ve hizmetlerin sunumu standartlaşmış olup, yüksek hacimlerde üretilebilmekte ve bu ürün ve hizmetleri sunan personelin de çok fazla niteliği olmasına gerek yokken, bazı ürün ve servislerin müşteriye istediği şekilde ulaştırılmasını belli düzeyde yetenek ve niteliğe sahip çalışanlar sağlayabilmektedir ve bunların üretimini ve sunumunu yapacak olan çalışanların ise karar verici ve inisiyatif alıcı olması beklenmektedir. Dolayısıyla, faaliyetin niteliğine bağlı olarak görev tanımları ve nitelikler şekillendirilmelidir.

Görev, yetki ve sorumlulukların tanımlanması, işlerin ve iş akışlarının tanımlanması kadar önemli bir noktadır. Görevlerin yeniden yapılandırılmasındaki amaç, işin gerektirdikleriyle çalışanların yeteneklerini uyumlu hale getirmektir. Eğer personelin yetenekleri ve tecrübesiyle işin gerekleri arasında bir uyumsuzluk varsa, bu personelin gerekli performansı gösteremeyeceğinin işareti olduğu gibi zaman zaman yetenek ve tecrübesine oranla çok basit işlemlerin gerçekleştiriliyor olması da personeli olumsuz yönde etkileyerek işten ayrılmalara sebebiyet verebilir.

Günümüzdeki anlayış değişikliğine karşın önceden, işin mümkün olduğunca parçalara ayrılarak standartlaşmış bir ürün ve servis üretimiyle maliyetlerin daha etkin bir

[145] Christopher Lee Marshall, **Measuring And Managing OPERATIONAL RISKS in Financial Institutions: Tools,Techniques and Other Resources**, Singapore: John Wiley&Sons, 2001, s.347-348.

şekilde kontrolü önemliydi [146]. Bu tür bir standartlaşmanın her zaman istenen sonuçları vermemesine bağlı olarak çalışanların görev tanımları ve yaptıkları işlerin zenginleştirilmesi amacıyla, daha önceye kıyasla farklı sorumlukların yüklenmesi, belirli bir rotasyon çerçevesinde değişiklik sağlanması ve böylelikle de personelin moral ve motivasyonunun artırılması amaçlanmıştır. Personelin görev tanımlarına bazı farklı görevler, sorumluluklar ve yetkiler ekleyerek iş tanımları daha zengin hale getirilebilir. Bu kapsamda rotasyon programları geliştirilip birimler arası belirli periyotlarda geçiş sağlanabilir. Özellikle personelin moral motivasyon eksikliğinden, iş tatmininin azalmasından kaynaklanan operasyonel riskler bu tür tedbirler ile azaltılabilir.

İş tanımının zenginleştirilmesinin bir sonraki aşaması, çalışanın nitelikleri, ilgi duydukları, başarılı bir şekilde gerçekleştirebildikleri ve inisiyatif kullanabilmesi göz önünde bulundurularak personelin kuruma daha fazla değer sağlayabilmesi amacıyla personelin özlük haklarında yapılacak iyileştirmeye paralel olarak iş tanımının genişletilmesi daha esnek bir yapıya kavuşturulmasıdır. Personelin görev, yetki ve sorumluluklarındaki artışın maddi olarak da desteklenmesi gereklidir. Aksi taktirde artan iş yükü ve sorumluluk moral ve motivasyonda ters yönde bir etki yaratıp memnuniyetsizliği de arttırabilir.

İş tanımlarını ve iş süreçlerini yeniden yapılandırırken dikkat edilmesi gerekli olan diğer bir husus ise görevler ayrılığı ilkesine bağlı kalmaktır. Görevler ayrılığını tesis edebilmek için, işlevsel görev ayrımlarının yapılması, çift taraflı ve çapraz kontrol ve imza mekanizmalarının oluşturulması, aynı kişide hem işlem yapma hem de muhasebeleştirme yetkisinin bulunmaması, işlemi yapan ile onaylayanın farklı kişiler olması gerekliliği yerine getirilmelidir[147]. Örneğin, ATM'lere para nakli yapılması gerektiğinde mutlaka iki kişinin nakil esnasında bulunması gereklidir, ya da belli bir tutarın üzerinde gişeden para çekilişi gerçekleşecek ise gişe de görev yapan personelden daha fazla tecrübesi olan bir onay biriminin olması operasyonel hataları azaltacaktır. Görevler ayrılığı sadece aynı fiziksel alanı paylaşan personel arasında olmak zorunda değildir. Örneğin, bazı bankalar şubelerce satışı yapılan bir kredinin kullandırılmasını şubeden değil genel müdürlükte bulunan merkezleştirilmiş operasyon birimlerinden gerçekleştirebilmektedirler. Bunun

[146] Marshall, s.358-361.
[147] Gürdoğan Yurtsever, "Bankacılıkta Personel Suiistimalerinin Önlenmesi ve Tespiti", **Active**, Sayı.46, 2006, s.46.

sebebi de kredilendirme sürecinde şubede olması gereken görevler ayrılığı ilkesinin işletilebilirliğini, kredi tahsisinde şube etkisini arındırarak kesinkes tesis etmektir.

2.2.3. İşe Alma ve Yerleştirme

İşe alma ve terfiye ilişkin olarak etkin şekilde işleyen insan kaynakları yönetimi, düşük ve verimsiz çalışma performansı, işten ayrılma oranın yüksek olması, çalışan kaynaklı hırsızlık ve zimmet olayları gibi kayıp ve risklerin önlenmesi için önemli bir noktadır. Çünkü etkin işleyen bir insan kaynakları politikası, çalışanların çalışma koşullarının iyileşmesini, iş tatmininin artmasını, personelin kendini geliştirmesini ve eğitmesini, çalışanlar arasında uyumlu bir ortamın doğmasını ve ödüllendirme mekanizmasının doğru ve dürüst bir şekilde işlediğine dair inancı kuvvetlendirdiği gibi düşük verimliliği, hatalı işten çıkarmaları, devamsızlığı, gereksiz yere iş yüküne maruz kalmayı da azaltmaktadır[148].

Kurumda insan kaynakları yönetiminin işleyişindeki etkinsizlik, işten ayrılma oranlarındaki artışla ilişkili olabilmekte ve kuruma ciddi maliyetler yükleyebilmektedir[149]. Çünkü, üzerinde yatırım yapılan, kurumu ve işleyişi anlaması zaman alan personelin işten ayrılması kurumlar için bir maliyet unsuru olduğu gibi çalışanlar arasında olması gereken takım ruhunun oluşmasını, köklü bir kurumsal kültürün tesis edilmesini ve gelecek dönemlere aktarılmasını da engellemektedir. İşten ayrılan personel sayısı ve oranının yüksek olması diğer personelin kuruma olan bağlılığını etkileyebilmekte, onların da farklı iş arayışlarına girmesine sebep olabilmekte, hatta kurumun kalıcı müşteri ilişkileri tesis etmesini engelleyebilmektedir.

Genel olarak iş dünyasında iş tecrübesi henüz fazla olmayan personelin daha tecrübeli personele göre ve bayan çalışanların erkek çalışanlara göre daha sık bir şekilde işten ayrıldığı düşünülmektedir. Kurum açısından her ne kadar işten ayrılmalar maliyet yaratsa da özellikle yüksek pozisyonlarda yer alan personelde görülen işten ayrılma sıklığı kurum için daha fazla maliyetlidir. Ama diğer taraftan da, personel değişim hızının çok yavaş olması da kurum için risk unsuru oluşturabilir. Çünkü, yeni bilgi ve becerilere sahip genç çalışanlar ile takviye edilmeyen kurumların performansında bir düşüş görülebilir.

[148] Chapman, s.230.
[149] Şebnem Acuner, "İnsan Kaynaklı Davranışşal Riskler ve Kuruluşlara Maliyeti", **Active**, May-Haz 2006, s.1.

Benzer şekilde, yönetici pozisyonlarında yeterince değişiklik olmaması, başarılı ve yüksek performans gösteren çalışanların kurum içinde yükselmesini zorlaştıracaktır. Böyle bir gelişme de verimli ve başarılı çalışanların motivasyonunun azalmasına, kariyer beklentilerinin gerçekleşmemesine, hatta kurumdan ayrılmalara kadar gidebilecek; kurum içerisinde yeni ve yaratıcı fikirlerin ortaya çıkmasını, değişimin uyarıcı etkisinin hissedilmesini engelleyecek ve çalışanların statükocu bir rahatlığa alışmalarına neden olabilecektir.

Personel kaynaklı bir diğer risk noktası ise çalışanlar tarafından gerçekleştirilen, çeşitli zimmet ve hırsızlık olaylarıdır. Bunun için, çalışanların geçmiş tecrübeleri, nitelikleri, bildirmiş olduğu bilgilerin doğruluğu ve tutarlılığı kontrol edilmelidir. Kurum, aynı zamanda personel tarafından yanlış ve yalan bildirimlere ilişkin izleyeceği politikayı net bir biçimde personele işe alım sürecinde bildirmiş olmalıdır[150].

Birçok kurumda işe alma ve terfi yüksek oranda mülakatlar sonucunda gerçekleşmektedir ve mülakatların gerçek anlamda bir çalışanın gelecekte göstereceği performansını, yeteneklerini, davranışlarını ve karakterini tam anlamıyla anlamak konusunda yeterli veriyi sağlamadığı da bir gerçektir[151]. Personelin seçiminin etkin bir şekilde gerçekleşmesi, çalışanın karakteri ve yetenekleriyle işin gerektirdiği niteliklerin ne ölçüde örtüştüğüne bağlıdır. Bunun için, personel seçiminde ve terfisinde öncelikli olarak söz konusu işin kapsamlı bir analizi gerçekleştirilmelidir. Organizasyonda yapılacak işlerin tanımlanması ve işi yapacak kişide aranan özelliklerin tespit edilmesi "iş analizi" olarak tanımlanır. İş analizinin içinde işin tanımı ve özellikleri, işi yapacak kişide aranacak özellikler, verilecek görev ve işin değerlendirmesi yer alır.

İnsan kaynakları yönetiminde en önemli görevlerden birisi de işe uygun elemanların alınması ve işe yerleştirilmesi işlemidir. Bunun için öncelikli olarak iş tanımında, organizasyondaki işler belirlenmeli, bu işlerin tanımı yapılmalı ve işi yapacak kişinin görev ve sorumlulukları açık olarak belirtilmeli ve bu işi gerçekleştirecek olan

---

[150] Yurtsever, s.47.

[151] Marshall, s.331-333. Ayrıca, iş görüşmelerinin etkinliği ve sağlılık olup olmadıkları üzerine 1929 yılında yapılan ve bu alanda ilk araştırmalardan biri olan Hollingsworth'un çalışmalarında 12 satış müdürünün mülakat sonrası işe alınacak aynı kişi hakkında son derece farklı değerlendirmelerde bulundukları saptanmıştır. www.makalem.com "Eleman Seçme ve Değerlendirme Teknikleri" s.1.

personelde olması gereken nitelikler ve aranan özellikler iş tanımında belirlenmelidir[152]. Kapsamlı bir şekilde iş analizi gerçekleştirilirken daha önce aynı pozisyonda görev alan personelin en iyi uygulamaları da değerlendirmeye alınmalıdır. Personel seçimi yaparken, adayların yetkinliği ve kapasitesini anlayabilmek için yetenek testleri oluşturulmalıdır. Aynı şekilde, zeka testleri ve kişilik testleri de etkin personel seçiminde kullanılan işlevselliği yüksek yöntemlerdir. Fakat bu tür testlerin dikkatsizce seçilmesi ve oluşturulması neticesinde verimsiz ve istenmeyen sonuçlara da ulaşılabilmektedir.

İşe alınacak elemanlar için yukarıda belirtilen temel bilgi ve becerilerin tespit edilmesinde mutlaka bazı ilkelerin olması gereklidir ve bu ilkelerin mümkünse organizasyonda yazılı hale getirilmesinde yarar bulunmaktadır. Çağımızın ünlü yönetim uzmanlarından Peter Drucker, organizasyonda işe alma ve yerleştirmede şu kriterlerin dikkate alınmasının önemi üzerinde durmaktadır[153]:

1- En uygun eleman işe alınmalıdır. Farklı görevler farklı özelliklere, beceri ve yeteneklere sahip kişilerin işe alınmasını gerektirir.

2- Potansiyel olarak işe uygun elemanlar arasından seçim yapılmalıdır. Etkin bir karar için potansiyel olarak birbirine yakın beceri ve kabiliyete sahip olan kişiler arasından seçim yapılmalıdır.

3- İşe alınacak adayları değerlendirirken çok iyi ve etraflıca düşünülmelidir. İşe alınması planlanan kişilerin sahip olduğu güçlü ve zayıf yönler iyi analiz edilmelidir. Teknik bilgi itibariyle yeterli olan bir aday işin gereği eğer organizasyonda grup çalışmasını yönetecek kapasiteye ve özelliklere sahip değilse o kişinin işe uygun olduğu söylenemez.

4- Her adayı daha önce birlikte çalıştığı kimselerle birlikte değerlendirmek gereklidir. Bir tek yöneticinin değer yargıları anlamsız ve değersiz olabilir. Bu bakımdan mümkün olduğu takdirde adayın durumu daha önceki yöneticileri ve çalışma arkadaşları ile görüşmeler yaparak değerlendirilmelidir.

---

[152] Kate Keenan, **The Managment Guide to Selecting People**, Sussex:Ravette Books, 1995, s.6-15.
[153] http://www.kendinigelistir.com/peter-druckerin-hayatindaki-7-onemli-ders/ (12 Mayıs 2007), s.122-125.

5- İşe alınan elemanın işten anlayıp anlamadığı ilk aylarda kontrol edilmelidir. Adaylar arasından seçim yapıldıktan sonra işin sona erdiği düşünülmemelidir. Çalışmaya başlayan elemana yardımcı olunmalı ve iş hakkındaki durumu değerlendirilmelidir.

6- Kuruma yeni alınan personele yapacağı görevle uyumlu bir eğitim programı uygulanmalıdır. Her unvanın/görevin gerektirdiği eğitim seviyesi, niteliksel özellikler önceden yazılı olarak belirlenmeli ve bunlar işe alınacak çalışanlar için göz önüne alınmalıdır.

Kurumda her birim için her yıl periyodik olarak bir norm kadro çalışması yapılmalı ve bu üst yönetime onaylatılmalıdır. Böylece organizasyonda her birim için mümkün olduğunca işin gerektirdiği sayıda kişinin çalıştırılması sağlanmış olacaktır.

2.2.4. Eğitim

Kurum tarafından gerçekleştirilen eğitimlerin bir çok amacı vardır. Bu eğitimler vasıtasıyla, kurumun riskleri nasıl değerlendirdiği ve nasıl yönettiği, buna ilişkin yaklaşımının nasıl olduğu, eğitim programının ve konusunun içinde yer alır ve personelin yapacağı işe uygun olarak yetkinlik seviyesinin geliştirilmesi hedeflenir. Kurumsal eğitimler bu amaçlara hizmet edebilmesi için, öncelikle kurum içinde eğitim ihtiyacının tespit edilmesi gereklidir. Daha sonra bir “Eğitim Planı” hazırlanarak eğitimin amacı, uygulanacak eğitim programlarının adı ve kapsamı, eğitim verilecek birimlerin ve personelin kimler olduğu, eğitim süresi, yeri, maliyeti, sonuçları gibi konular belirlenmelidir. Eğitim planının tespitinden sonra eğitim programlarının uygulanması konusunda ilkelerin belirlenmesi gereklidir. Kurumda eğitim iş başında olabileceği gibi iş dışında da olabilir. İş dışında eğitim, eğitim programlarını uygulayan yönetim danışmanlığı firmalarından ya da eğitim konusunda uzmanlaşmış eğitim kuruluşları ile işbirliği yapılarak gerçekleştirilebilir.

Eğitim plan ve programları hazırlanırken kurumda her kademede çalışanlara yönelik eğitim ve seminer uygulanmasına özen gösterilmelidir. Eğitimler sadece teoride kalmamalı, uygulamaya yönelik olmasına da özen gösterilmelidir. Çalışanların eğitimlere katılımı ve başarısı izlenerek değerlendirilmeli, verilen eğitimin sağladığı fayda ölçülmeli, değerlendirilmeli ve sonuçları örneğin personelin performansında, terfisinde dikkate alınmalıdır. Asgari her yıl yapılan anketlerle birimlerin eğitim ihtiyacı sorgulanmalı, eğitim

programları düzenli olarak gözden geçirilmelidir. Eğitim eksikliği nedeniyle yapılan işlemlerde hata oluşması halinde, bu eksikliğe dönük eğitimler planlanmalıdır.

Risk yönetimi kapsamında personele verilen eğitim, personele olası kayıplar ve bu tür kayıpları analiz etme, ölçme ve bu riskleri yönetmeye dönük gerçekleştirilen faaliyetleri anlatmalıdır. Örneğin, hazinede ön ofiste ya da bankacılıkta şubede satış kısmında çalışan bir personelin sahip olduğu nitelik ve tecrübe, olası operasyonel kayıplara karşı önemli bir süzgeçtir. Risk yönetimine ilişkin belirli birimlerde ve pozisyonlarda oluşabilecek risklere karşı spesifik eğitimler verilmeli, bu tür eğitimlerin içeriği kapsamı ve yoğunluğu ise personelin mevcut tecrübesine, gerçekleştirdiği işin risklilik derecesine göre değişmelidir.

Terfi veya parasal ödüllerle sağlanan motivasyon kurumun eğitim politikasının etkin olabilmesi için büyük önem taşımaktadır[154]. Kurumun personelinin eğitimine net bir şekilde önem verdiğinin tüm çalışanlarca bilinmesi motivasyon için gereklidir. Sektörde rekabetin sağlanabilmesi açısından personelin sektörel eğitimlerden uzak kalmaması gereklidir. Sektörel eğitimlerle edinilen ve/veya kurum içinde birikmiş olan tecrübe, kurum içi eğitimlerle, intranet üzerinde kurulacak portallar ile veya diğer iletişim araçlarıyla tüm personele aktarılmaya özen gösterilmelidir. Ayrıca çalışanların kariyer hedeflerinin yöneticilerce bilinmesi ve belirlenen ortak hedefler doğrultusunda onlara kendilerini geliştirme imkanı sağlanması da motivasyon artırıcı unsurlar arasında sayılabilir.

2.2.5. Yetki Kullanımı

Günümüzde artık fiziken gelen/giden az sayıdaki evrak haricinde operasyonel işlemlerin büyük çoğunluğu tam otomasyon içerisinde gerçekleşmektedir. Bu durumda ister istemez sistemsel yetki kullanımı tüm kurumlarda büyük önem taşımaktadır. Kurumun bir program menü envanteri çıkartılmalı ve programlara erişim, verilecek yetkilerle sağlanmalıdır.

Programların rapor ekranları ile operasyonel işlem ekranlarına erişim mümkünse farklı seviyedeki yetkilendirme prosedürleriyle sağlanmalıdır. Böylece programları izleyen, operasyonel işlem yapmayan örneğin iç sistem birimleri personeli ile operasyonel işlem

[154] Marshall, s.333-334.

yapan birim personelinin yetkilendirmesinde sorun yaşanmayacaktır. Yetkilendirme menü adımları personelin görev tanımları ile de uyumlu olmalıdır. Kendi yetkisinde veya görev ve sorumluluğunda olmayan personelin kendi yetkisinde olmayan işlere erişimi engellenmelidir. Personelin görev değişikliği, terfi gibi nedenlerle ortaya çıkan yetki değişiklikleri hemen gözden geçirilmelidir. Bir çalışanın görevden ayrılması halinde zaman geçirmeden yetki iptali yapılmalıdır. Bunun için kurum içerisinde oturmuş bir süreç ve yazılı prosedürler olmalıdır.

2.2.6. Çalışanların Motivasyonu

İnsan kaynakları yönetiminin en önemli konularından birisi hiç şüphesiz motivasyon yönetimidir. Motivasyon, kısaca insanı çalışmaya sevk etmek, çalışmak için bireyi harekete geçirmek ve isteklendirmek anlamına gelmektedir. Motivasyon yönetimi ise organizasyonda çalışanların daha istekli ve arzulu iş yapmalarına yönelik çeşitli araçlar (para, eğitim, takdir, ödüllendirme, başarı vs.) ile çalışanların harekete geçmesi ve isteklendirilmesi demektir[155].

Motivasyon eksikliğinin operasyonel riskin kaynaklarından biri olduğu ortadadır. Bunun için, çalışanların memnuniyet seviyesi periyodik aralıklarla ölçülmeli ve değerlendirilmelidir. Çalışanların memnuniyeti doğrultusunda performansı ve verimliliği arttırıcı çalışmalar yapılmalıdır. Motivasyon konusundaki yaklaşımların temeli ödüllendirme beklentisine dayalıdır. Birey göstereceği çabanın takdir edilmesi ve ödüllendirme beklentisi içerisindedir. Eğer organizasyonda takdir ve ödüllendirme ile ilgili ilkeler ve politikalar önceden belirlenmiş ise bu çalışanlar üzerinde motive edici etki gösterecektir. Motivasyonda organizasyonda uygulanan ödüllendirme sisteminin adil olması da elde edilen sonuç açısından önem taşımaktadır. Eğer organizasyonda uygulanan ödüllendirme sistemi adil ise bu durumda kişilerden elde edilecek sonuç olumlu olacaktır. Kişiler ya aynı tempoda çalışmayı sürdüreceklerdir veyahut da daha yüksek performansla çalışacaklardır. Eğer organizasyonda uygulanan ödüllendirme sistemi adil değilse o zaman da yapılan işte tatminsizlik, verimlilikte azalma, düşük performans, işten ayrılmalar gibi durumlar söz konusu olabilecektir. Yukarıda bahsedilen ödüllendirme tanımı sadece parasal anlamda bir artı değer sağlamaktan ötedir; çünkü çalışanların motivasyonunu belirleyen en temel

[155] http://www.canaktan.org/yonetim/insan-yonetim/motivasyon-teorileri.htm (17 Haziran 2008)

etmen aldıkları ücret değildir. Yapılan bazı araştırmalar[156] çalışanların aldıkları ücretin iş tatmini sağlamada üçüncü sırada yer aldığını göstermektedir. İş tatminini etkileyen en önemli iki faktör yönetimin denetleme-kontrol uygulamaları ve kariyer-gelişim fırsatlarıdır.

Çalışanların motivasyonu artıran önemli diğer bir faktör ise kurumun amaçlarının, hedeflerinin ve bunlara ulaşmak için gereken araçların belirlenmesinde çalışanların da belirli ölçülerde bu sürece dahil edilmesidir. Çünkü, kurumsal hedef ve amaçlar saptanırken ve bazı kararlar alınırken çalışanların katılımlarını sağlamak çalışanların kuruma bağlılığını arttıran bir faktördür. Yapılan araştırmalara[157] göre; işin hızı, görev dağılımı, yapılacak işle ilgili fazla mesai gerektirip gerektirmediği, verilecek dinlenme araları gibi işyeri kuralları konusunda çalışanların fikrinin alınması ve kararlara katılımlarının sağlanmasıyla, ahlaki değerler ve iş doyumunda artış, devamsızlıkta ve çatışmalarda azalma ve işi bırakma sayısında düşüş görülmüştür.

2.2.7. Performans

Performans değerlendirmesi, iş hedeflerine ve davranışlara odaklanılması, çalışan motivasyonunun artırılarak gelecekteki kişisel ve kurumsal performansın yükseltilmesi açısından çok değerli bir fırsattır ve kurumun risk yönetiminin etkinliğinin dolaylı olarak belirleyicilerinden birisidir.

Çalışanların performanslarının değerlendirilmesi ve ölçülmesinin amacı, insan kaynaklarının organizasyon amaçlarına ne ölçüde katkıda bulunduğunun tespit edilmesidir. Kurumlarda, insan kaynaklarında performans değerlendirme ve ölçmesinin çeşitli amaçları vardır. Bunlar genel olarak[158]; organizasyonda çalışan personel arasındaki performans farklılığını ödüllendirmek, daha fazla çalışma gayreti içerisinde olan personeli motive etmek, ücret artışı ve terfileri daha rasyonel ve objektif temellere dayandırmak, performans değerlendirilmesinin ardından “geri bildirim” ile kişinin kendi kendinin performansını değerlendirebilmesini sağlamak ve kurumdaki eğitim ihtiyacını tespit etmek ve en genel

[156] Smith, (17 Haziran 2008), s.2.
[157] Acar Baltaş, **Değişimin İçinden Geleceğe Doğru Ekip Oluşturma ve Liderlik**, İstanbul:Remzi Kitapevi, Aralık 2000, s.170-173.
[158] Can Aktan, “2000'li Yıllarda Yeni Yönetim Teknikleri: İnsan Mühendisliği”, İstanbul: TÜGİAD Yayını, 1999.

anlamda da kişisel ve kurumsal performansın yükseltilmesi açısından kurumun risk yönetiminin etkinliğinin artırılmasını sağlamaktır.

Performansa dayalı ücret sistemi, ücret ile performans arasında ilişki kurularak oluşturulan ücret sistemleridir. Bir başka ifadeyle çalışanlara, işin değeri yerine, çalışanların yarattığı değerlere (performans düzeylerine) göre ücret ödemeye dayanır. Çalışanların ve kurumun performansını artırmada yaygın olarak kullanılan bir araç olan bu yöntem, daha yüksek bir çaba düzeyini beraberinde getirerek performans düzeyinin yükselmesini sağlamaktadır[159].

Eğitim ihtiyaçlarının belirlenmesinden kariyer gelişimine yön verilmesine kadar bir çok insan kaynakları uygulamasına girdi sağlayan performans değerlendirmesinin organizasyonların başarısı için çok kritik olduğu kabul edilen ve eksikliğinin operasyonel riskin kaynaklarından biri olduğu bilinen "çalışan motivasyonu" üzerinde önemli etkileri olduğu bilinmektedir. Çalışanların çalıştıkları kurumu sahiplenmeleri, işten ayrılma oranlarının azalması, üstün performans gösteren çalışanların kurumda çalışmaya devam edebilmesi ve kurumsal hedeflerin gerçekleştirilebilmesi için kurumlar performans değerlendirmesini daha stratejik bir konuma yerleştirmektedir.

Performans değerlendirmesi ve ölçülmesi çalışanların motivasyonu ile birebir ilişkili bir konu olup çok dikkatli ve mümkün olduğunca objektif esaslara göre işleyen bir süreç olmalıdır: Örneğin, performans yönetim sistemine ilişkin politika ve prosedürler belirlenerek yazılı hale getirilmiş olmalı, çalışanlara işe ilişkin hedefler açık bir şekilde bildirilmeli, performans kriterleri gerçekleştirilen işle ilgili olmalı ve özel hayata ilişkin ayrıntılı değerlendirmelere yer verilmemelidir. Ayrıca, performans değerlendirme kriterleri tespit edilirken amacın başarıyı tanımak ve ödüllendirmek olduğu unutulmamalı ve ücret ve/veya terfi politikaları çalışanların performansı ile uyumlu olmalıdır. Performans değerlendirme kriterleri tespit edilirken çalışma sonuçlarının ölçülmesine özen gösterilmelidir. Örneğin, işe devam durumu, işe geç kalma sıklığı, yapılan işin kalitesi, bilgi ve beceri düzeyi, izin alınan gün sayısı, üretim sürecinde kişinin kendisinden kaynaklanan hata oranı vs. kriterler ölçülebilir bazı performans göstergeleridir. Bunun dışında çalışanın

[159] Mehmet Hüseyin Bilgin, "Bireysel Performansa Dayalı Ücret ve Verimlilik", http://www.econturk.org/Turkiyeekonomisi/cmis1.pdf (12 Haziran 2009).

liderlik ve yöneticilik yeteneği de performans değerlendirme ve ölçülmesinde dikkate alınmalıdır. Aynı şekilde çalışma grupları içerisinde uyum ve işbirliği dahilinde çalışma durumu da dikkate alınmalıdır. Kurum çalışanlarının performanslarının değerlendirilmesinde müşterilerin çalışanlar hakkındaki şikayetlerini de dikkate almakta fayda vardır[160].

Diğer taraftan etkin yürütülmemiş bir performans değerlendirmesinin motivasyon üzerinde olumsuz etkileri olduğu da göz ardı edilmemelidir. Yapılan tüm değerlendirmeler ve verilen geribildirimler, kişinin duyguları, tutumları, alışkanlıkları ve değerlerinin yansıması olan davranışlarına yöneliktir. Kişilerin özgüveninin sarsılmaması ve saldırgan bir tavır almaması için bu hassas dengelerin gözetilmesi gerekir. Aksi takdirde çalışanın motivasyonunun düşmesi kaçınılmazdır. Nitekim, organizasyonlarda performans değerlendirme süreci, genellikle çalışanlar ve yöneticiler arasında ilişkilerin gerildiği, sancılı bir dönemi de beraberinde getirir. Etkili yürütülmeyen bir performans değerlendirme, performans sorunları ve kişisel sorunların karıştırıldığı karmaşık bir ortamın doğmasına sebep olabilir. Bu durumun yan etkisi olarak, çalışanın işe karşı motivasyonunun düşmesinin yanı sıra, çevresindeki çalışma arkadaşları da bu tür sorunlardan etkilenecek ve genel anlamda da operasyonların etkin ve hatasız bire şekilde gerçekleşmesinde bazı sorunlar ortaya çıkabilecektir.

Performans değerlendirme sırasında üzerinde durulması gereken bir başka konu da değerlendirilen kişiden beklentilerin gerçekçi olması ve çalışana başarabileceği hedeflerin verilmesidir. Çünkü gerçekleştirilen hedeflerin beraberinde getirdiği başarı hissi çalışanda motivasyonun artmasına ve uzun vadede kurumun daha fazla yarar sağlamasına neden olacaktır. Geri bildirimlerin sürekliliği de değerlendirmelerin çalışan motivasyonu üzerindeki etkisi açısından önemli bir konudur. Üstlerin astlarına değerlendirme dönemi boyunca gerektiği zaman geri bildirim vermemesi, dönem sonu değerlendirmelerinde çalışana baş edebileceğinden daha fazla sorumluluğun verilmesine, performansının ve motivasyonun düşmesine neden olabilir. Bu sebeple, geri bildirimler, etkinliğin artırılması açısından gerektiğinde gözlemlenen davranışların hemen ardından verilmeli ve performans değerlendirme görüşmesinin yapılacağı zaman beklenmemelidir.

[160] Zuhal Akal, **"İşletmelerde Performans Ölçüm ve Denetimi; Çok Yönlü Performans Göstergeleri"**, Ankara: MPM Yayını, 1992.

2.2.8. Suiistimal ve Dolandırıcılık

Suiistimal ve dolandırıcılık kapsamı, yalan söylemek veya küçük hırsızlıklardan büyük zimmet suçlarına kadar bir çok insan kaynaklı riski içermektedir. Suiistimal ve dolandırıcılık, kurumda çalışan en alt düzeydeki personelden en üst düzeyde görev yapan yöneticilere kadar farklı profildeki çalışanlar tarafından gerçekleştirilebileceği gibi, kurum içinde çalışmayan ama kurumla ilişkisi olan müşteriler ve tedarikçilerce de gerçekleştirilebilir. Suiistimal ve dolandırıcılık ile ilgili olarak akla ilk gelen ve medyada geniş yer bulan olaylar bankalarda yaşanan zimmete geçirmeler ve personel kaynaklı suiistimallerdir. Genelde, yönetici konumundaki personel tarafından gerçekleştirilen dolandırıcılık olayları kamuoyuna yansısa da daha alt seviyede görev alan personel tarafından gerçekleştirilen ufak boyutlu suiistimallerin sayısı ve toplamı da önemlidir. Örneğin, alt seviyelerde görev alan personel tahrif edilmiş harcama belgelerini kullanarak, kurumun iş ilişkisinde bulunduğu alıcı ve satıcılardan ufak tutarlarda çeşitli menfaatler temin ederek, kuruma ait eşya ve malzemeleri özel işlerinde kullanarak veya çalarak belirli ölçüde suiistimal gerçekleştirmiş olabilir. Diğer taraftan, yönetici pozisyonundaki çalışanlar ise mali tablolarda maddi hatalara sebebiyet vererek kar, satış, maliyet rakamlarını değiştirerek veya kurumun iş yaptığı ve anlaşma sağladığı büyük sözleşmelerin tesis edilmesi sürecinde kişisel menfaat sağlayarak suiistimal gerçekleştirmiş olabilirler. Suiistimallerin oluşmasının arkasında bazen muhasebeye dönük kontrollerin zayıf olması, çalışanlar ile kurum personeli olmayan kişiler arasındaki çıkar çakışması veya bazen de, ne gibi durumda kurum personelinin nasıl davranması gerektiğini net bir şekilde ortaya koyan etik değerler kılavuzunun olmaması neden olabilmektedir.

Suiistimal ve dolandırıcılığa karşı etkin mücadele en başta doğru personel seçiminde ve insan kaynakları uygulamalarında başlamaktadır. İşe alım sürecinde, adayların geçmişlerinin ayrıntılı ve mümkün olduğunca farklı kaynaklardan araştırılması, belirttiği tecrübe ve eğitim bilgilerinin doğruluğu ve tamlığının çapraz kontrollere tabi tutulması, kişinin mümkünse mali borçluluk durumu ve kredi istihbaratının gerçekleştirilmesi, tutarlı ve kapsamlı kişilik testlerinin uygulanması önemlidir ve buna bağlı

olarak adayların hangi nedenlerle işe kabul edilemeyeceğini tanımlayan tutarlı bir politikanın tesis edilmesi gereklidir[161].

Suiistimal ve dolandırıcılığı önlemek için süreçlerde görevler ayrılığı prensibi en etkin şekilde tesis edilmelidir. Bu prensip, gerçekleştirilen bir operasyonel işin en az başka bir kişi tarafından kontrol edilerek sağlanabilir. Örneğin, hazine bölümünde alım-satım operasyonu yapan kişi ile, gerçekleşen işlemlerin muhasebe kayıtlarını girenlerin farklı kişiler olması veya kurum alacaklarını ve borçlarını takip eden sorumluların ayrı olması gibi uygulamalar görevler ayrılığı prensibine uygun oluşturulmuş süreçler olup suiistimalleri engellemeye dönük yapılanmalardır. Yine diğer taraftan, kritik öneme sahip personel sayısını uygun bir düzeyde tutmak, söz konusu personeli zaman zaman çapraz görevlerde çalıştırarak rotasyona tabi tutmak, en az on, onbeş gün kesintisiz yıllık izin kullanmalarını sağlamak konusunda ısrarlı olmak gibi uygulamalar suiistimallerin önlenmesi konusunda önemli noktalardır.

Suiistimallerin tespit edilebilmesi için, etkin bir iç kontrol sisteminin tesis edilmesi, iç ve dış denetimlerin düzenli olarak gerçekleştirilmesi gerekmekle birlikte yine de çoğu zaman suiistimaller şans eseri ortaya çıkarılmaktadır[162]. Suiistimallerin tespiti ve önlenmesi öncelikle yeterli sayıdaki denetçiden oluşan etkin bir iç denetim sistemi ile mümkündür. Fakat Çok sık şekilde gerçekleştirilen denetimler personel üzerinde tam ters bir etki yaratarak personelin moral ve motivasyonunu da olumsuz biçimde etkileyebilir. Bunun için, etkin bir denetim ve kontrol sisteminin yanına personelin suiistimalleri tespit edebilmesine olanak sağlayan kurum içi eğitimlerin sağlanması, kurumsal olarak uygulanacak etik değerler setinin yayınlanması ve asıl olarak da mümkün olduğunca iç kontrole dönük faaliyetlerin operasyonel iş süreçlerinin içine entegre edilmesi ve işletilmesi gerekir. Böylelikle, olası risklerin zamanında fark edilmesi ve önlem alınması mümkün olabilecektir[163].

Personel kaynaklı riskleri önceden tespit edebilmek için bazı göstergelerden faydalanılabilir. Örneğin, personelin izin kullanım sıklığı ya da kullanmaması personelden

[161] Gürdoğan Yurtsever, "Bankacılıkta Personel Suiistimalerinin Önlenmesi ve Tespiti", **Active**, Sayı.46, 2006, s. 47-48
[162] Marshall, s.369-373.
[163] Yurtsever, s.45.

kaynaklanabilecek olan riskler için öncü bir göstergedir. Çünkü, kurum içinde bazı suiistimaller gerçekleştirmiş olan bir personel sürekli olarak işe gelmek isteyecek, gerçekleştirmiş olduğu suiistimalin ortaya çıkmasına olanak sağlayacak tüm yoları kapamaya çalışacaktır. Bunun için, tüm personelin yıllık izinlerini kullanmaları zorunlu olmalıdır. Bazen de, çalışanların durum ve davranışlarındaki belirgin değişiklikler bazı suiistimal olaylarının habercisidir. Örneğin, işe zaman zaman geç gelen bir personelin artık işe çok daha erken gelmeye başlaması, ya da tam tersi, veya bir personelin çok sayıda operasyonel hata yapmaya başlaması ya da personelin özel hayatında olan ve maddi sebeplerle açıklanamayan önemli değişiklikler olası suiistimallerin işareti olabilir.

Suiistimalleri önlemek için yukarıda anlatılan öneriler kısaca şu şekilde özetlenebilir: Kurumda çalışanların karşılaştığı problemleri ve şüpheli gördükleri hususları (dolandırıcılık, suiistimal vb risklerin azaltılmasına yönelik olarak) anında rapor etmelerini sağlayacak süreçler mevcut olmalı ve merkezi denetim, geçici hesap kontrolü, kredi limit ve teminat bilgililer kontrolü gibi suiistimalleri önleyici erken uyarı mekanizmaları kurum içinde iş süreçlerinde ve organizasyonel yapıya tesis edilmelidir. Yine, suiistimal olması halinde uygulanacak politika, prosedür, işlem ve cezalar yazılı olarak belirlenmiş ve tüm çalışanlar bu konularda bilgilendirilmiş olmalıdır. Ayrıca, usulsüz işlemler sonucu uygulanan yaptırımların caydırıcılığı periyodik olarak gözden geçirilerek gerekli düzenlemeler yapılmalıdır. Diğer taraftan ise, usulsüz işlemlere karşı çalışanlara eğitim verilmesi, şifrelerin gizliliğinin korunması gibi yöntemlerle proaktif önlemler alınmış olmalıdır ve kurum izin politikasını risk yönetiminin bir parçası haline getirmelidir ve bu kapsamda çalışanların izin konusu önceden belirlenmiş kurallara bağlı olmalı, personelin en az 2 hafta kesintisiz izin kullanım zorunluluğu uygulanmalıdır.

2.2.9. Kurumsal Kültür

Operasyonel risk kapsamında kurumsal kültür, bir şirketin günlük operasyonel faaliyetlerine yön veren değerler, amaçlar, pratikler ve davranışların oluşturduğu bir değerler setidir[164]. Diğer bir ifadeyle, kurumsal kültür, bir kurumun temel faaliyetlerine arka planda yön veren değerler ve normlar setidir ve bir işletmenin geçmişinden ve iş yapma şeklinden bire bir etkilenir. Kurumun sahip olduğu felsefe aynı zamanda kurum kültürünün

[164] Chapman, s.241.

önemli bileşenlerinden biri olan risk yönetim felsefesini belirler ve bu çerçevede de tüm kurumca paylaşılan, stratejileri belirlemekten tutun da günlük operasyonel faaliyetlerin ne şekilde gerçekleştirileceğine kadar kurumun riski nasıl tanımladığını gösteren, böylelikle de ortak değerler ve davranışları belirleyen kodlar ve normları oluşturur. Dolayısıyla kurumsal kültür, kurumun değerlerini yansıtır, kültürünü ve operasyonel işleyişini belirler ve örneğin, risklerin nasıl tanımlanacağı, ne tür risklerin kabul edilip ne şekilde yönetileceği gibi risk yönetimini oluşturan diğer ana parçaların nasıl uygulanacağını etkiler.

Operasyonel kayıpları önlemenin araçlarından birisi de operasyonel riske ilişkin farkındalıkları kurumsal kültürün bir parçası haline getirmektir[165]. Bunun için operasyonel riskin önemi konusunda personelin eğitilmesi gerekmektedir. Operasyonel risk yönetimini kurumsal kültürün bir bileşeni haline getirmek için personelin gerekli eğitim ve formasyonu edinmesi sağlanmalı, operasyonel risk performans ölçümünde ve bonus-ikramiye ödüllendirmesinde parametre olmalıdır[166]. Kurumsal kültür, her ne kadar personel tarafından günlük operasyonel faaliyetlerin yürütülmesindeki yaklaşımların üzerinden kazanılsa da zaman zaman çeşitli eğitimler ile de desteklenmelidir. Çünkü, kurumun sahip olduğu kültürel kodlar işe yeni başlayan personele veya kurumun iş yaptığı taraflara günlük operasyonel işleyiş içinde hissettirilir. Normlar ve yaklaşımlar, grup olarak hareket etmeyi kolaylaştırdığı gibi kuruma yeni dahil olan personel de çevresindeki diğer personelin tutum ve davranışları doğrultusunda kurumsal kültürü algılayabilir. Kurum içinde bireylerin davranışları ve olaylara yaklaşımları personelin kurumsal kültürle ne ölçüde uyumlu hareket ettiğine bağlı olarak değişkenlik gösterebilmektedir. Kurumun sahip olduğu kültürel yapısı ile risk yönetimine bakışı arasında da önemli bağlantılar vardır. Risk yönetimi, bir anlamıyla kurumun her bir seviyesinde görev alan personelin davranış ve faaliyetlerinin olumlu bir toplamını yansıtır.

Risk yönetim felsefesi, tüm çalışanlarca en iyi şekilde anlaşılıp, uygulandığı ve benimsendiği ölçüde kurum riskleri tespit edip etkin bir şekilde yönetme konusunda daha güçlü bir konumda olabilecektir[167]. Kurumun farklı birimleri ve farklı yöneticileri risk yönetimi

---

[165] Hussain, s.112.
[166] Hübner ve Diğerleri, s.20-22.
[167] Committee of Sponsoring Organizations of the Treadway Commission (COSO), **Enterprise Risk Management Integrated Framework, Executive Summary Framework,** New York:AICPA, September 2004, s.27-28.

karşısında ortak bir felsefeden hareket etmiyorlarsa ortak bir felsefenin kurumca uygulandığından söz edilemez. Her ne kadar, kurumun gelişmiş bir risk yönetim felsefesi olsa da kültürel farklılıklar, birim yöneticilerin riske karşı farklı tolerans seviyelerinin olması ve risk iştahlarının farklılık arz etmesi gibi sebeplerden dolayı kurumsal risk yönetiminin kurumca tek düze bir şekilde uygulanması zor olacaktır. Bazı birim müdürleri riske karşı daha esnek tanımlar geliştirirken, bazıları daha muhafazakar risk tanımları oluştursa kurum içinde yer alan bu tür birimsel farklılıklar kurum performansını olumsuz etkileyebilir. Örneğin, iddialı satış hedefleri olan satış departmanı hedeflerine ulaşmak için riski daha esnek tanımlayabilecekken, sözleşmeleri düzenleyen hukuk departmanı yasal mevzuata uyum konusunda oldukça dikkatli davranabilecektir. Fakat, birimler birlikte çalışarak, kurumun risk yönetim felsefesini uygun ve makul bir biçimde faaliyetlerine yansıtabilirler.

Bir kurumun işleyişine temel oluşturan kültürel kodları değiştirmek hiç de kolay bir iş değildir. Çünkü mevcut kültür bu tür bir değişime direnecektir. Örneğin, eski kurumsal yapıda olmayan açıklık, şeffaflık gibi bazı kavramların ön plana çıkması gerekecektir[168]. Çünkü, etkin risk yönetimi için personelin risk unsuru, zafiyet, eksiklik olarak gördüğü noktaları her hangi bir çekinme olmadan üst yönetimle görüşebiliyor olmalıdır. Benzer bir yaklaşım her hangi bir kaybın yaşandığı ya da gerçekleşmekte olduğu anlarda da geçerlidir. Kurumsal kültürü değiştirmek amacıyla önerilen klasik yöntem üç aşamalıdır[169]: öncelikle mevcut kalıplaşmış, donmuş olan kültür "çözülmeli", ardından yeniden yapılandırma süreci işlemeli ve en son olarak yeni kültürel yapı tekrar dondurulmalıdır. Bir kurumda kültürel bir değişim yaşanacaksa, bu süreç genellikle yaşanan bir kriz sonrasında oluşur ve öncelikle böyle bir durumda yönetim değişikliği meydana gelir. Yeni gelen yönetim, kurumsal kültürü yenilemek ve değişime sokmak amacıyla, oyunun kurallarını yeniden yazmaya çalışır. Bu kültürel değişimin kurumun temel strateji ve hedefleriyle uyumlu olması gereklidir ve bunun için zaman zaman yönetim değişikliği, maddi ve maddi olmayan haklar ve ücretlendirmede olumlu yönde artışlar, terfi veya yeni personel alımı, kontrol ve denetim süreçlerinin daha etkin ve kapsamlı hale getirilmesi gibi politikalar uygulanabilmektedir. En son olarak da yeni kültürel kodların belirli bir süre için "dondurulması" gerekir ki bu sürecin tüm kurum seviyesinde hem personelin moral ve

[168] Haubenstock, s.258.
[169] Marshall, s.335-337.

motivasyonu üzerinde hem de kurumun genel verimlilik ve operasyonel risklilik düzeyi üzerinde etkileri olur. Kültürel değişim aynı zamanda, kurumlara belirli ölçüde maliyet de yaratmaktadır. Bu süreçte yeni yapılanmaya alışamayacak olanlar ayrılmak zorunda kalabildiği gibi belirli birimlerde olumlu yönde gelişim sağlayacak olan değişim belki başka birimlerde ya da faaliyet gösterilen farklı coğrafyalarda olumsuz bir uyum ve bütünlük sorununa yol açabilecektir.

2.2.10. Normlar ve Limit Uygulaması

Kurallar ve limitler, kaçınılması gereken riskleri tanımlayarak belirlenen sınırların aşılması durumunda uygulanacak olan müeyyideleri belirlerler. Kurumca yayınlanmış olan etik değerler, risk politikaları, uygulama talimatları veya gişe/hazine/kredi tahsis limitleri gibi referanslar tipik olarak norm ve limitleri ifade eder. Bu tür sınırlar ve normlar özellikle büyük ölçekli kurumlarda gereklilik olarak ortaya çıkmaktadır. Çünkü geniş bir kurumsal yapılanmada personeli ve faaliyetlerini bireysel ilişkiler vasıtasıyla kontrol etmek mümkün olmayacağına göre belirli işlevsel sınırlar ancak bu tür limit ve normların tesis edilmesi ve etkin bir şekilde uygulanması ile sağlanabilir. Bu tür limit ve sınırlar, personelin kuruma önemli riskler yükleyebileceği birimlerde ve işlerde daha hassas bir şekilde belirlenmelidir.

Normlar ve limitler geliştirmenin esas amacı, belirli sınırlar dahilinde kişilere serbest oyun alanları ve inisiyatif yaratmaktır[170]. Eğer operasyonel bir faaliyet riskli ise, kurumun risk toleransına göre ve işin risklilik durumuna göre gerekli olan sınır ve limitler belirlenmelidir. İdeal olan, belirlenen limitlerin optimum seviyede esnekliği barındırması ve çeşitli noktalarda inisiyatif kullanabilmeye olanak sağlamasıdır. Çünkü, limitlerin belirlenmesinde iki önemli unsur rol oynar[171]. Öncelikle mutlak anlamda alt ve üst limitler ne olmalıdır ve ikincil olarak da limitlerin aşımı ve yönetimi konusunda hangi kişilere ne kapsamda yetkiler verileceğidir. Alt ve üst limitler, bir kurumun maruz kalabileceği risklerin olasılık ve etkileri üzerine tahminlere dayanarak belirlenmelidir. Olasılığı düşük de olsa etki düzeyi ne kadar yüksekse maruz kalınabilecek böyle bir riskle ilgili olarak düşük bir limit seviyesi belirlenmelidir. İkincil olarak da risk yönetimi konusunda hangi personele ne tür inisiyatif noktaları verileceğidir. Geniş yetkiler geniş sorumluluklar anlamına gelir ve geçmiş

[170] Marshall, s.390-392.
[171] Carl Olsson, **Risk Management in Emerging Markets**, 1.Baskı, London:Prentice Hall, 2002, s.118-119.

iş tecrübesi, eğitimi ve donanımı göz önünde tutularak sadece belirli derecede güven kazanmış çalışanlara bu kapsamda yetkiler tanımlanır.

Limitlerin yönetiminde dikkat edilmesi gerekli olan bir başka nokta da aşımların nasıl yönetileceğidir. Bu tür aşımlar sadece kurumun operasyonel faaliyetlerinde daha dikkatli hareket etmesine işaret olup, her aşımın en kısa zamanda normal seviyesine çekilmesi gereklidir. Bu tür aşımlar sehven olabildiği gibi, zaman zaman bir onay mekanizması içerisinde ilgili yöneticinin de haberinin olduğu durumlarda ortaya çıkabilmektedir. Limit aşımında önemli olan, aşım sınırlarının hiç bir şekilde ihlal edilmemesi olmayıp sadece faaliyetlerin risklik durumlarına göre bazı operasyonların ve işlemlerin daha dikkatli bir şekilde takip edilmesinin sağlanmasıdır.

Limit yönetiminin daha etkin işleyebilmesi için zaman zaman personele daha önceden tanımlanmış olan limitlerin söz konusu personelin iş tecrübesine ve mesleki bilgisine bağlı olarak revize edilmesi olanaklı olmalıdır. Ayrıca, limitleri belirlemenin bir diğer yönü ise, uygunsuz faaliyetlerin kolay ve maliyetsiz bir şekilde tespit edilebilerek söz konusu sınırlar ve normlar aşıldığı zaman bu tür sınırlamaları aşanların ne çeşit bir yaptırıma maruz kalacakları net ve açık bir şekilde önceden politika haline getirilmesidir.

2.2.11. Görevler Ayrılığı ve Çift Kontrol

Görevler ayrılığı aslında Adam Smith'e kadar giden kavramlara dayanır: Eğer çalışanlar belli bazı işlerin ve görevlerin yerine getirilmesinde uzmanlaşırsa ve tecrübe kazanırsa, her işin herkes tarafından yapıldığı yapılanmalara kıyasla daha iyi sonuçlar ortaya çıkar. Görevler ayrılığını tesis etmenin bir diğer ve asıl önemli sebebi ise farklı ve belli noktalarda birbiriyle içerik olarak çelişebilecek işlerin farklı kişilerce yapılmasının sağlanması ile olası suiistimallerin önlenmesidir[172]. Örneğin, bir kurumun satışlarını ve alışlarını aynı kişi kayıt altına alıyor ve üst yönetime raporluyorsa bu noktada doğal olarak suiistimal ihtimali artmaktadır. Çünkü, gerçeklemiş olan alışları hiçbir şekilde kurumun stoklarına almadan satış gerçekleştirirse ve bu satışları da kayıt altında gerçekleştirmezse kurum kaybetmiş, ama personel kazanmış olur. Alım sürecinde satın alma birimi gelen stoktan daha az bir tutarı kayıtlarına yansıtmak istemeyeceği gibi yine stoklardan sorumlu

[172] Brink, s.95.

olan departman da kendilerine teslim edilenden daha fazla stoğu kayıtlarına yansıtmayacaklardır.

Finansal kurumlarda ise para ve mal akışını kontrol etmek ve ayırmak ise daha zordur. Çünkü bankalarda para aslında perakende sektöründeki mallar gibidir. Parasal tüm transferlerin sistem üzerinden gerçekleştirilebildiği finansal kurumlarda görevler ayrılığı ancak yazılım destekli kişisel şifrelerle sağlanabilir. Örneğin, bankacılıkta kredi tahsisi iki bacaklı bir iş akışında gerçekleştirilir. Pazarlama portföyü kredi talep eden müşterinin başvurusunu sistem vasıtasıyla değerlendirir ve kredi kullandırılabilir bir müşteriyse gerekli teminatlar tesis edildikten sonra müşterinin istediği tutar hesabına başka bir personel tarafından transfer edilir. Kredi kullandırımını gerçekleştiren personel gerekli teminatların tesis edilmediğini görürse krediyi kullandırmaz. Gerçekleştirmesi gerekli olan belirli satış hedefleri bulunan pazarlama portföyü gerekli teminatları tesis etmeden, hatta suiistimal amaçlı olarak da fiktif şahıslar üzerinden, kredi kullandırımını gerçekleştirebilir ki kurumu çok ciddi risk altına sokabilir.

Çift kontrol, operasyonel riskleri azaltmak anlamında görevler ayrılığının tesis edilmesi ilkesine benzese de kontrolleri gerçekleştiren personel arasında doğal bir çıkar çatışması olmak zorunda değildir. Veri girişlerinde, düzeltmelerde, iptallerde girişi gerçekleştiren ve onu kontrol eden kişinin ayrı olması operasyonel hataların oluşmasını engellemeyi amaçlar. Yine kurumu yasal olarak temsilen üçüncü taraflara verilen yazı ve belgelerde çift imzanın olması, kurumun itibarını korumaya dönüktür. Çift taraflı kontrol şu iki şekilde gerçekleştirilebilir: öncelikle, bir çalışan tarafından girilen data diğer bir personel tarafından kontrol edilir; ikincil olarak da sistem ikinci personelin datayı girmesini ister ve ilk girilen data ile tutarlılığını kontrol eder. Her ne kadar, ikincil olan yöntem çok daha güvenli ise de uygulaması ve kurumca gerçekleştirilmesi daha pahalıdır.

2.3. Sistem Kaynaklı Operasyonel Riskler ve Yönetimi

Operasyonel risk yönetimini kaynaklarına göre sınıflandırmak gerekirse, sistem kaynaklı risklerin yönetimi bu kapsamda ele alınıp *“Bilişim Teknolojilerinde Risk Yönetimi”* olarak adlandırılabilir. Risk yönetimi genel anlamda, bir kuruluşu risklere karşı kontrol etmek ve yönlendirmek amacıyla, belirlenen hedeflere ulaşmak için yürütülen süreçleri

destekleyen ve kurumun kritik varlıklarını koruyan bir yaklaşımdır. Bu sürecin en önemli unsuru da belirlenen risk toleransına göre fayda/maliyet dengesini hep göz önünde bulundurmaktır[173].

Günümüzde teknolojinin inanılmaz hızda gelişimi, sunulan ürün ve hizmetlerdeki çeşitliliğin artması gibi faktörler iş süreçlerini karmaşık hale getirmekte, denetimi zorlaştırmakta ve sonuç olarak kurumların hata, dolandırıcılık gibi tehditlere karşı tedbirlerini önceden almalarını zorunlu hale getirmektedir. Zira organizasyonlar açısından bilişim teknolojilerine dayalı süreçler, asli işlevlerini, varlıklarını devam ettirmeleri açısından büyük önem arz etmektedir.

"TS ISO/IEC 27001:2005 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler" standardına göre risk yönetimi bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler olarak tanımlanmıştır. Risk yönetimi, bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla koruyucu önlemlerin maliyetlerinin dengelenmesi ve organizasyonun hedeflerine ulaşması için gerekli kritik sistemlerin korunması gibi konularda BT yöneticilerinin yararlandığı süreçtir. Bu süreç risk analizi, risk işleme ve değerlendirme ve takip alt süreçlerinden oluşmaktadır[174].

Organizasyonlar, öncelikle bünyelerinde risk yönetim sisteminin kurulmasını da kapsayan Bilgi Güvenliği Yönetim Sistemini (BGYS) oluşturmalıdırlar. Bu sistem, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenmesi gereken ve kurumun personelini, iş süreçlerini ve bilgi teknolojilerini kapsayan sistematik bir yaklaşımdır. Bilgi güvenliğinin sağlanabilmesi için bilginin gizliliğinin (confidentiality) yani yetkisiz kişilerin erişimine kapalı olmasının, bilginin bütünlüğünün (integrity) yani yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasının, bilginin

[173] Thomas R. Peltier&Justin Peltier, **Complete Guide to CISM Certification**, New York: Auerbach Publications, 2006, s.69.
[174] Doğan Eskiyörük, "BGYS – Risk Yönetim Süreci Kılavuzu", **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00,17/08/2007, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0004-bgys-risk-yonetim-sureci-kilavuzu.html (16 Haziran 2008), s.6.

kullanabilirliğinin (availibility) yani ihtiyaç anında kullanıma hazır durumda olmasının yeterli düzeylerde sağlanması gereklidir[175].

Bilgi Güvenliği Yönetim Sistemi deyimi ilk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Daha sonra bu standart Uluslararası Standartlar Kurumu ISO tarafından kabul edilmiş ve ISO/IEC 27001:2005 olarak yayınlanmıştır. BSI tarafından yayınlanan ve yine ISO tarafından kabul edilerek ISO/IEC 27002:2005 olarak bilinen bir diğer standart BS 7799-1 ise bilgi güvenliğinin sağlanmasında kullanılacak kontrollerden bahsetmektedir.

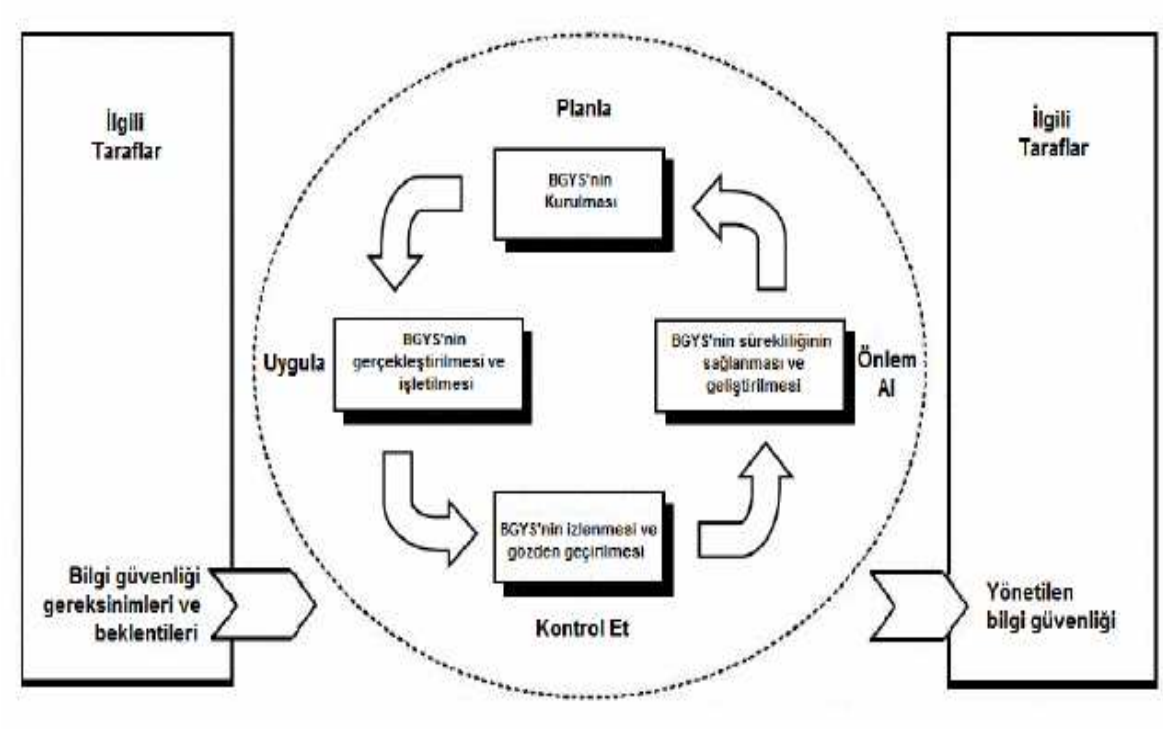
Bir kurumda BGYS'nin kurulumu öncelikle üst yönetim tarafından benimsenmelidir. Üst yönetimin bu sistemin gerekliliğine ve faydasına inanması, onun başarısının birincil şartıdır. Başarıdaki diğer önemli husus, BGYS'nin kurumun iş yapma tarzını etkileyen bir sistem olduğunun tüm kurum çalışanlarınca benimsenmesi ve tüm iş süreçlerinde bu bilinçle hareket edilmesidir. Hatta etkin bir BGYS kurulumu için, kurum çapında her birimden ilgililerin katılımından oluşan "Bilgi Güvenlik Komisyonu" nun oluşturulmasının faydalı olacağından bahsedilmektedir. Komisyon temsilcileri bilgi güvenliği konusunda deneyimli, bilgili ve kendi bölümlerini temsil edebilme yetkinliğine sahip olmalıdırlar[176].

BGYS standartları kapsamında BGYS'in kurulumu, gerçeklenmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi için PUKÖ (Planla - Uygula -Kontrol et - Önlem al) modeli kullanılmaktadır. PUKÖ modelini görsel olarak anlatan Şekil 5, bir BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini göstermektedir.

Bilgi güvenliği yönetimi, başlangıç ve bitiş tarihleri olan bir proje gibi görülmemelidir. Sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ

[175] Dinçer Önel ve Ali Dinçkan, "Bilgi Güvenliği Yönetim Sistemi Kurulumu" **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00,28/08/2007, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulum-kilavuzu.html (16 Haziran 2008), s.6-7.
[176] Önel ve Dinçkan, s.10.

modelinde gösterildiği gibi faaliyetleri bir döngü içinde durmaksızın sürekli devam etmelidir. BGYS'nin kurulması toplam on adımdan oluşan bir süreçtir. Aşağıda bu adımlar sırasıyla açıklanmaktadır.



Şekil 5: BGYS Süreçlerine Uygulanan PUKÖ Modeli

Kaynak: Dinçer Önel ve Ali Dinçkan, **"Bilgi Güvenliği Yönetim Sistemi Kurulumu"** TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Sürüm 1.00,28/08/2007, http://www.bilgiguvenligi.gov.tr, (16 Haziran 2008),s.6-7.

2.3.1. Adım 1: Kapsam Belirleme

Faaliyetler, organizasyonel birimler, işin mekanı, varlıklar ve teknoloji karakteristikleri belirtilerek ve kapsam dışında kalacak olan her ayrıntının sebepleri

açıklanarak BGYS'nin sınırları ve kapsamı tanımlanmalıdır. Kurumda hangi birimlerin ve faaliyetlerin bilgi güvenliği yönetim kapsamı içerisinde yer alacağı belirtilmelidir[177].

Kapsam dokümanı çok sık değişime uğraması gerekmese de yaşayan bir dokümandır. Gerektiğinde kapsamın içeriği değiştirilebilir. Fakat kapsamın ilk aşamada belirlenirken yönetilebilir boyutta tutulması önemlidir. Bu yüzden organizasyonun fiziksel yapısı ve süreçleri göz önüne alınmalıdır. BGYS'nin kapsamı kurumun belli bir kısmı olabileceği gibi, kurumun bütünü de olabilir. Ancak, her iki durumda da, kurumun BGYS kapsamını ve sınırlarını eksiksiz ve doğru bir biçimde tanımlaması gerekmektedir. Örneğin sadece kurum içindeki bir bölüm veya bir bölümün verdiği tek bir hizmet için de bir BGYS hayata geçirilebilir. Örneğin; az görülmesine rağmen yönetilebilirlik adına çok büyük bazı organizasyonlarda finans bölümü ve yazılım geliştirme bölümü için iki ayrı BGYS oluşturulduğu gibi örnekler mevcuttur[178].

BGYS kapsamı, üst yönetimin niyeti ve kurumun bilgi güvenliği hedefleri dikkate alınarak belirlenir. ISO/IEC 27001 ve ISO/IEC 27002 standartlarının bu konuda belli bir yönlendirmesi veya zorlaması söz konusu değildir. Kapsam belirlenirken BGYS dışında bırakılan varlıklarla ve diğer kurumlarla olan etkileşimleri de dikkate almak gereklidir. Kapsam dışında bırakılanların hangi sebeplerle dışarıda bırakıldıklarını kurumun sağlam gerekçelerle açıklayabilmesi gerekmektedir. Bu adımın sonunda bir kapsam dokümanı yayınlanmalı ve üst yönetim tarafından onaylanmalıdır.

2.3.2. Adım 2: BGYS Politikası

Kapsamın belirlenmesinin ardından gelen adım BGYS politikasının oluşturulmasıdır. Bilgi güvenliği politikaları, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür[179]. Bu kural ve uygulamaları tanımlayan politikalar çeşitli

---

[177] R.Saliba, “Callio Secura 17799- A tool for Implementing the ISO 17799/BS 7799”, 1998, s.12-14’den Ünal Perendi**,** “BGYS Kapsamı Belirleme Kılavuzu”, **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00, 21/03/2008, http://www.bilgiguvenligi.gov.tr (16 Haziran 2008), s.6.

[178] Ted Humphreys, “ISMS Standarts The ISO 27000 Family and BS7799-2”**, ISMS International User Group Seminar**, s.32-35’den Ünal Perendi, s.6.

[179] Tuğkan Tuğlular, "Üniversitelerde Bilgi Güvenliği Politikaları"**, Ulaknet Sistem Yönetimi Konferansı - Güvenlik**, Ekim 2003’den Günce Öztürk, “Bilgi Güvenliği Oluşturma Kılavuzu”, **TÜBİTAK UEKAE:Ulusal**

seviyelerde yazılabilir. Politikalar, genel bir bilgi güvenliği politikası ve belirli alanlara ait politikalardan (erişim kontrol politikası, uzaktan erişim politikası, kullanıcı politikası, e-posta kullanım politikası vb.) oluşup uygulamaları tanımlayan prosedür ve talimatlarla tamamlanabilir.

Her seviyedeki politikanın tek bir dokümanda bulunması yerine, en üst seviyede temel ilkeleri barındıran bir Bilgi Güvenliği Politikası'nın oluşturulması ve bu dokümanla diğer ayrıntılı politikaların ilişkilendirilmesi tavsiye edilmektedir[180]. Bu politika, hedefleri ortaya koyan, yönetime yön veren ve harekete geçiren, hangi riskin değerlendirmeye alınacağına ilişkin risk yönetim kapsamı ve kriterini belirleyen bir çerçeve sunmalıdır. BGYS politikasının amacını bulması için yönetim politika içeriğindeki maddelerin uygulamaya geçirileceğine ilişkin kararlarlığını çalışanlara hissettirmelidir. Bilgi Güvenliği Politikasında en azından aşağıdaki hususlar yer almalıdır[181]

a) Bilgi güvenliğinin tanımı, genel kapsamı ve hedefi,
b) Bilgi güvenliğinin kurum için neden önemli olduğu, bilgi güvenliği sağlanmasının amacı ve bilgi güvenliği ilkeleri, bu amaç ve ilkeler için yönetim desteği,
c) Kontrol hedefleri ve kontrollerin seçimi için risk değerlendirmesi ve risk yönetimini de içeren bir çerçevenin ortaya konulması,
d) Güvenlik politikaları, ilkeleri, standartları ve uyum gereksinimlerinin özet bir açıklaması,
e) Bilgi güvenliği ile ilgili tüm görev ve sorumlulukların tanımı,
f) Diğer ayrıntılı politikalar ve belirli bilgi sistemleri için prosedürler veya kullanıcıların uyması gereken kurallar gibi politikayı destekleyen dokümanlara atıflar

---

Elektronik ve Kriptoloji Araştırma Enstitüsü, Sürüm 1.00, 21/03/2008, http://www.bilgiguvenligi.gov.tr (16 Haziran 2008), s.6.

[180] Scott Barman,**Writing Information Security Policies**, New Riders Publishing, 2001'den Günce Öztürk, s.6.

[181] Ted Humphreys ve Angelika Plate, **Guide to the Implementationn and Auditing of ISMS Controls based on ISO/IEC 27001**, British Standards Institution, 2005'den Günce Öztürk, s.7.

2.3.3. Adım 3: Risk Değerlendirme Yaklaşımı

Bilgi güvenliği politikası temel alınarak sistematik bir risk değerlendirme yaklaşımı belirlenmelidir. Kurum kendine uygun bir metodoloji seçmekte serbesttir. Seçilen risk değerlendirme metodolojisi kıyaslanabilir ve tekrarlanabilir sonuçlar üretmeyi garanti etmelidir. Bu adımda kabul edilebilecek risk seviyeleri yani kurumun risk toleransı belirlenmeli ve bunlar için ölçütler geliştirilmelidir. Özellikle BS 7799-3 standardı risk değerlendirme konusunda geliştirilmiş bir standarttır[182].

Risk yönetiminde esas olan, riskin tümüyle engellenmesi değil, sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesidir. Başarılı bir risk yönetimi için, kurumun varlıklarına ve hedeflerine yönelik riskleri belirlemek, analiz etmek, denetim altında tutmak ve izlemek gereklidir[183].

Risk değerlendirmesi çalışmasında aşağıdaki esaslar göz önünde bulundurulmalıdır[184]:

a) Bilgi varlıklarının (ekipman, yazılım vb.) ya da iş varlıklarının ve aktivitelerinin tanımı ve değerinin tespit edilmesi,
b) Bu varlıklara karşı, içeriden veya dışarıdan gelebilecek tehditlerin belirlenmesi,
c) Bu tehditlerin oluşma olasılığının belirlenmesi,
d) Bu tehditlerin kurumdaki etkilerinin belirlenmesi,
e) Tehditlerin engellenmesi veya kabul edilebilir bir seviyeye indirilmesi için gerekli ek kontrollerin belirlenmesi,
f) Ek kontrollerin uygulanması için aksiyonların planlanması.

2.3.3.1. Varlıkların Belirlenmesi

Varlık bir kurum için değer taşıyan, sistemin bir parçası olan ve bu nedenle korunması gereken tüm unsurlardır.

---

[182] Önel ve Dinçkan, s.11-12.
[183] "Bilişim Teknolojilerinde Risk yönetimi"**, TBD Kamu-BİB Kamu Bilişim Platformu VIII**, 2.Çalışma Grubu Raporu, Belge No: ÇG2/Sürüm4, http://www.kamubib.tbd.org.tr/dokumanlar/CG2S.doc (22 Mart 2007), s.11.
[184] "Bilişim Sistemleri Güvenliği El Kitabı"**, TBD Kamu-BİB Bilişim Platformu**, http://kamubib.tbd.org.tr/dokumanlar/bg2.doc (22 Mart 2007), s.12.

İnsan, bilgi, yazılım, donanım, bina, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir. Örneklerde verilen varlıklar içerisinde en soyut olanı bilgidir. Bilgi bir organizasyonda her yerde bulunabilir. Donanımlar ve yazılımlar bilgiyi işler, donanımlarda ve medyalarda (CD, USB depolama üniteleri) depolanır, dokümanlarda yazılı olarak bulunur. Kurum çalışanlarının zihinlerinde, konuşmalarında bulunur.

Varlıkların türleri ve bu türlere örnekleri aşağıda yer almaktadır[185].

a. **Bilgi varlıkları:** Kurumun tüm bilgi sistemlerinde, çalışanlarında, kütüphanelerinde tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen veridir. Örneğin veritabanları, veri dosyaları, sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri, iş süreklilik planları vs. gibi.

b. **Yazılım varlıkları:** Uygulama yazılımları, ofis programları, sistem yazılımları, geliştirme araçları ve yazılımları.

c. **Fiziksel varlıklar:** Bilgisayar ekipmanları (kasa, işlemciler, ekranlar, diz üstü bilgisayarlar, modemler), manyetik kayıt ortamları (teyp, kartuş, kayıt cihazları ve diskler), diğer teknik araçlar (güç kaynakları, havalandırma üniteleri), mobilya, yerleşim düzeni.

d. **Servisler (Hizmetler):** Bilgi işleme ve haberleşme servisleri (web servisi, e-ticaret servisi, ftp servisi), genel hizmetler(örneğin ısınma, ışıklandırma, elektrik, havalandırma).

e. **İnsan:** Kurum personeli de kurumun beyin gücü olarak kurum varlığı olarak düşünülmelidir.

Yukarıda bahsi geçen varlıklar kurum içerisinde BT sistemini kullanan, tasarlayan ve destekleyen personele uygulanacak anketlerle, BT sistemini yöneten veya bu sisteme destek sağlayan personel ile yapılacak birebir görüşmelerle, önceki yıllara ait risk değerlendirme raporlarının, kurum politikaları ve sistem dokümantasyonunun incelenmesiyle, ağ tarama araçları gibi otomatik arama yapan bir program vasıtasıyla veya bunlara benzer yöntemlerle kolayca belirlenip Tablo 10'da yer alan benzer bir envantere işlenebilirler.

[185] Fatih Koç, "BGYS – Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu", **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0003-varlik-envanteri-olusturma-kilavuzu.html (20 Mart 2008), s.6.

Tablo 10: Örnek Bir Varlık Envanter Tablosu

Sıra No	Varlık Grubu	Varlığın Tanımı	Modeli	Markası	Kategori	Varlık Sahibi	Varlık Emanetçisi	Gizlik Değeri	Bütünlük Değeri	Erişilebilirlik Değeri	.....	Açıklama
1												
2												
..												

Kaynak: Fatih Koç, **"BGYS – Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu"**, TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Sürüm 1.00, 20/03/2008, http://www.bilgiguvenligi.gov.tr, (16 Haziran 2008), s.6.

2.3.3.2. Varlıkların Sınıflandırılması

Varlık envanteri oluşturulduktan sonra varlıkların önem derecesine göre sınıflandırılarak kurumun varlıklarına değer biçilmesi risk analizi için temel bir adımdır. Tüm varlıklar belirlendikten sonra ikinci adım olarak, bir varlık için değer atama kriterinin belirlenmesi gerekir. Varlık çeşitleri düşünülecek olursa, değer atama kriteri belirlenmesi kurumdan kuruma çok değişiklik göstermektedirler. Kimi varlıkların değeri nicel olarak atanabilirken (rakamsal ifadeler kullanılarak) kimi varlıklar için ise nitel tanımlar kullanılabilmektedir (düşük, çok yüksek gibi).

Varlık derecelendirmesi/değerlemesi yapılırken objektifliğin sağlanabilmesi için (derecelendirme sonucunda farklı kişilerin aynı varlığa aynı veya yakın bir dereceyi ataması için) doğru bir metodoloji uygulanması gereklidir. Bu metodoloji organizasyon için

varlık sınıflandırma kılavuzuna temel teşkil edecektir[186]. Örneğin kurum varlıklarından bilgi varlıkları Tablo 11'deki kategorilere göre sınıflandırılabilir:

Tablo 11: Bilgi Varlıklarının Sınıflandırılması

KATEGORİ	AÇIKLAMA
Çok Gizli	İzinsiz olarak açıklandığı takdirde kurumu finansal, operasyonel ve itibar imaj açısından olumsuz yönde önemli düzeyde etkileyebilecek, olağanüstü önem taşıyan bilgi varlıklarıdır. Çok gizli bilgi varlıkları, güvenliği sağlanmış ve sadece yetkili kişilerin girebileceği odalarda bulunan kasa ya da kilitli dolaplarda saklanmalı; kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir.
Gizli	Kurumun faaliyetini devam ettirebilmesi için kritik olan ve yetkisiz kişilerin eline geçmesi durumunda, sorunların yaşanacağı bilgi varlıklarıdır. Kasa ya da kilitli ortamda saklanmalı; kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir.
Kuruma Özel	Kurum dahilinde üretilen; yönergeler, talimatlar, standartlar, prosedürler, politikalar ve bu bilgilerin bulunduğu ortamlar vb. gibi, Kurum dışına çıkarılması için onay alınması gereken bilgi varlıklarıdır. Kurum içinde kullanımında, kopyalanmasında sakınca yoktur.
Hizmete Özel	Sadece belli bir grup tarafından, örneğin proje ekipleri, belli bir birim gibi, görülebilecek olan bilgi varlıklarıdır. İçerdiği konular itibarıyla, diğer gizlilik dereceli konular dışında olan, ancak güvenlik işlemine ihtiyaç gösteren bilgi varlıkları hizmete özel olarak sınıflandırılır. Gizli varlıklar gibi, yetkili kişi izni ile kopyalama, iletme ve imha işlemi yapılmalıdır.
Kişiye Özel	Sahibine özel kullanılan bilgi varlıklarıdır. Herhangi bir güvenlik derecesine sahip olmayan, iş ile ilgili ya da iş dışındaki bilgilerdir.
Halka Açık	Kullanılması güvenlik açısından önemli olmayan, herkese açık bilgilerdir.

Kaynak: "Bilişim Sistemleri Güvenliği El Kitabı", TBD Kamu-BİB Bilişim Platformu, Mayıs 2006, s.14-15

2.3.3.3. Varlıkların Etiketlenmesi

Kurumda varlık envanteri çıkartılıp bu varlıklar kritiklik seviyelerine göre belirlendikten sonra gerekli olduğu durumlarda fiziki ve elektronik ortamda olan bilgi varlıkları sınıflandırma derecesini gösterecek şekilde etiketlenmelidir. Etiketlendirmenin

[186] Koç, s.14.

nasıl yapılacağına ilişkin usul ve esaslar hazırlanacak bir prosedürde açıkça belirtilmelidir. Bilgi etiketleme ve işlemede aşağıdaki bulunan kurallar uygulanmalıdır[187].

a) **Fiziksel etiketler,** mümkün olduğu durumlarda kullanılmalıdır. Bununla beraber, elektronik biçimdeki belgeler gibi bazı bilgi varlıkları, fiziksel olarak etiketlenemezler. Bu nedenle, bu tür belgelerde elektronik anlamda etiketlemenin kullanılması gerekmektedir;

b) **Dokümanlar**, içerdiği bilginin en yüksek güvenlik seviyesi göz önüne alınarak sınıflandırılmalı ve bu sınıflandırma derecesi her sayfanın sol üst ve alt köşesinde büyük harflerle ve altı çizili olarak yer almalıdır;

c) **Manyetik kayıt ortamındaki (kartuş, disk, disket, CD, kaset vb.) bilgiler** yine en üst güvenlik seviyesi dikkate alınarak etiketlenmeli ve sınıflandırma seviyesi büyük harflerle ve altı çizili olarak medya üzerine yazılmalıdır;

d) **Elektronik ortamdaki belgelerde de (Word, Excel, Powerpoint dosyaları vb),** bilginin güvenlik seviyesini gösteren ibare, dosya içerisinde her sayfada sol üst ve alt köşede büyük harflerle ve altı çizili olarak bulunmalıdır;

e) **Çok gizli, gizli, hizmete özel bilgilerin** gerekli güvenlik önlemi alınmadan posta, faks veya elektronik ortamda aktarılmaması gerekmektedir. Yine bu seviyedeki bilgiler, izinsiz kişilerin eline geçme riski olduğundan, cep telefonu, sesli mesaj, telefon gibi ortamlarda aktarılmamalıdır;

f) **Çok gizli, gizli, hizmete özel güvenlik seviyesine sahip** bilgi varlıklarına sahip kişiler, bu varlığın bilmesi gerekenlerden başkasının görmemesini sağlamalıdır

2.3.3.4. Varlıkların Kullanımına İlişkin Prosedür Hazırlanması

Bilgi varlıklarının, sistem ve süreçlerinin kabul edilebilir kullanımı ile ilgili kurallar kurum tarafından dokümante edilmeli ve uygulamaya konmalıdır. Kabul edilebilir bilgi kullanımı kuralları çerçevesi içerisinde hangi sınıftaki bilgilerin hangi ortamlarda bulunabileceği, bu bilgilerin nerelerde saklanabileceği ve bu bilgilerin hangi şartlarda ve ne şekilde kimlerle paylaşılabileceği belirtilmelidir. Bu kurallar birlikte iş yürütülen yüklenici firmalar ve üçüncü parti organizasyonlar için olduğu kadar organizasyon çalışanları için de

[187] "Bilişim Sistemleri Güvenliği El Kitabı"**, TBD Kamu-BİB Bilişim Platformu**, http://kamubib.tbd.org.tr/dokumanlar/bg2.doc (16 Mayıs 2006), s.15.

uygulanmalıdır. Bu kurallar özellikle e-posta ve internet kullanımı, cep telefonu ve dizüstü bilgisayar ve kurumun sınırları ötesine ulaşan bilgi sistem ürünleri için düzenlenmelidir[188].

2.3.3.5. Tehditlerin Belirlenmesi

BT risk yönetim sürecinde varlıklar belirlenip varlık envanteri oluşturulduktan sonra, bu varlıkları olumsuz yönde etkileyebilecek, onların çalışmalarını tamamen veya kısmen durdurabilecek, onlara kasıtlı veya kazayla bir açıklığı kullanarak zarar verebilecek tehditleri belirlenir. Tehditler en genel anlamda Tablo 12'de belirtildiği gibi üç ana kategoride toplanırlar. Farklı risk yönetim metodolojileri bu sınıflandırmada farklı yaklaşımlar sergileyebilmektedir. Örneğin "OCTAVE" Metodolojisinde tehditler kaynaklarına göre "insan kaynaklı" ve "dış kaynaklı" olmak üzere iki grupta toplanmıştır[189].

Tablo 12: BT Tehdit Türleri ve Örnekler

TEHDİT TÜRÜ	ÖRNEK
Doğal tehditler	Deprem, sel, toprak kayması, yıldırım düşmesi, fırtına gibi tehditler.
Çevresel tehditler	Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vs.
İnsan kaynaklı tehditler	İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar. Örneğin yanlış veri girişi, ağ saldırıları, zararlı yazılımların yüklenmesi, yetkisiz erişimler vs.

Kaynak: Doğan Eskiyörük, **"BGYS–Risk Yönetim Süreci Kılavuzu"**, TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Sürüm:1.0, 17/08/2008, http://www.bilgiguvenligi.gov.tr, (16 Haziran 2008),s.8-9.

Kuruma özgü tehdit listesi varlık sahiplerinden, kullanıcılardan, BT uzmanlarından, kurumun korunmasından sorumlu kişilerden oluşan bir ekip tarafından oluşturulabilir. Tehdit değerlendirmesi sırasında hassas davranılması ve hiçbir tehdidin küçümsenerek göz ardı edilmemesi gerekir. Zira önemsiz olduğu düşünülüp göz ardı edilen bir tehdit beklenmedik düzeyde kurumun güvenliğinde zafiyet yaratabilir.

[188] Koç, s.15.
[189] Christopher Alberts and Audrey Dorofee, **OCTAVE Method Implementation Guide Vol.18 Appendix/E**, Pittsburgh: Carnegie Mellon Software Engineering Institute, 2003

2.3.4. Adım 4: Varlık – Tehdit Matrisinin Oluşturulması

Kurum içerisinde varlık envanteri, tehdit listesi oluşturulduktan sonra varlık-tehdit matrisi oluşturulmalıdır. Bu matriste bir tarafta kurumun BT varlıkları yer alırken diğer tarafta bu varlıklara etki edebilecek tehditler yer alır. Her bir varlığın maruz kalabileceği tehditler matriste işaretlenir. Örnek bir varlık-tehdit matrisi Tablo 13'de gösterilmektedir.

Tablo 13: Örnek Varlık – Tehdit Matrisi

		VARLIKLAR							
		PC'ler	**UPS Sistemi**	**Personel**	**Sunucular**	**Operasyonel Veriler**	**WAN-LAN Cihazları**	**Depolama Üniteleri**	**.....**
TEHDİTLER	**Hırsızlık**	☑	☑	☐	☑	☑	☑	☑	
	İşletim Sistemi Hatası	☑	☐	☐	☑	☑	☑	☑	
	Çevresel Felaketler (Deprem, Sel, vb)	☑	☑	☑	☑	☑	☑	☑	
	Güç Kesintisi	☑	☐	☐	☑	☑	☑	☑	
	Yazılım Hatası	☑	☐	☐	☑	☑	☑	☑	
	Mantıksal Yetkisiz Erişim	☐	☐	☐	☐	☑	☐	☐	
	Virüs/Worm/Trojan/Malware	☑	☐	☐	☑	☑	☐	☐	
	.....								

(☑: Varlık üzerinde tehdit mevcuttur. ☐:Tehdit varlığı etkilemez.)

Matris doldurulurken dikkat edilmesi gereken husus bir BT varlığının fiziksel özelliği ile içerisinde barındırdığı yazılım, işletim sistemi, veri gibi mantıksal kısmın ayrı ayrı sütunlarda tehdit değerlendirmesine tabi tutulmasıdır. Örneğin fiziksel bir varlık olarak PC, mantıksal varlık olarak içerisinde barındırdığı yazılımlar, işletim sistemi birbirinden ayrı sütunlarda BT varlığı olarak değerlendirilebilir. Böylece örneğin hırsızlık tehdidi PC'leri etkilemesine rağmen "Mantıksal Yetkisiz Erişim" tehdidi PC'lerin fiziki varlığını etkilemez ama PC'ler içerisinde yer alan yazılımları ve operasyonel veriyi tehdit eder.

2.3.5. Adım 5: Risklerin Belirlenmesi

Varlık – tehdit matrisi oluşturulduktan sonra sıra risklerin belirlenmesine gelir. Matriste yer alan ☑ şeklinde işaretlenmiş her bir varlık-tehdit eşleşmesi için ortaya çıkabilecek muhtemel riskler belirlenir. Bu tanımlamada ilgili tehdide karşı alınmış olan kontroller göz ardı edilerek kalıtsal (inherent) brüt riskler tanımlanmalıdır. Risk tanımlamalarında kurumun değerlendirmesi kapsamında çok daha detaylara inip, herhangi bir varlık-tehdit noktası için birden fazla risk tanımlaması yapmak mümkündür. Kurum bu değerlendirmeyi çok fazla detaya indirgemeyerek, genel anlamda da yapabilir. Bu nokta tamamen kurumun belirlediği politikaya bağlıdır.

Örneğin varlık:Muhasebe Müdürlüğü uygulama programları, tehdit:bu programlara yetkisiz mantıksal erişim olsun. Bu durumda ortaya çıkabilecek olası riskler aşağıdaki üç başlık altında toplanabilir.

1. Muhasebe uygulamalarına mantıksal yetkisiz erişim ile veri alımı,
2. Muhasebe uygulamalarına mantıksal yetkisiz erişim ile veri oluşturulması, değiştirilmesi,
3. Muhasebe uygulamalarına mantıksal yetkisiz erişim ile veri silinmesi

2.3.6. Adım 6: Brüt Risk Analizi ve Derecelendirilmesi

Matristeki varlık –tehdit eşleşmelerine ait tüm riskler belirlendikten sonra sıra tespit edilen risklerin analizi ve derecelendirilmesinin yapılmasına gelmiştir. Bu adım bir önceki adımda tespit edilen risklerin yorumlanması olarak da görülebilir. Risk analizi yaparken riske neden olan tehdit ve açıklıklardan yola çıkılmalıdır. Risk, açıklığın bir tehdit tarafından kullanılmasıyla oluşur. Örneğin duvarı delik bir ev düşünelim. Duvardaki delik açıklığı temsil eder. Olası bir sel ise burada tehdidi oluşturur. Bu ikisinin bir araya gelmesiyle risk oluşur ki bu örnekte risk evi su basmasından dolayı evdeki insanların veya eşyaların zarar görmesidir[190].

Riskin derecelendirilmesi veya değerinin belirlenebilmesi için öncelikle tehdidin gerçekleşme olasılığı ile varlık üzerindeki etki derecesi hesaplanmalıdır. Bunlar sayısal değerler kullanılarak hesaplanabileceği gibi rakamlarla ifadenin zor olduğu durumlarda

[190] Önel ve Dinçkan, s.12.

düşük, orta, yüksek, çok yüksek gibi nitel değerlerle de belirlenebilir. Tablo 14'de örnek bir olasılık-etki matrisi yer almaktadır.

Tablo 14: Olasılık-Etki Düzeyi Matrisi

BRÜT RİSK DÜZEYİNİN BELİRLENMESİ		ETKİ				
		1 ÖNEMSİZ	2 AZ ÖNEMLİ	3 ORTA ÖNEMLİ	4 ÖNEMLİ	5 ÇOK ÖNEMLİ
OLASILIK	5 Olması kesin veya sık sık gerçekleşmiş- Normal çalışma şartlarında (Olasılık >= %50)	O	Y	Y	ÇY	ÇY
	4 Olması oldukça muhtemel veya zaman zaman gerçekleşmiş-Sıklıkla (%50> Olasılık >= %10)	O	O	Y	Y	ÇY
	3 Olması muhtemel veya seyrek olarak gerçekleşmiş-Az(%10 > Olasılık >=%1)	D	O	O	Y	Y
	2 Olması İhtimali Çok Düşük -Çok az (%1 > Olasılık >= %0.1)	D	D	O	O	Y
	1 İmkansız veya olması muhtemel değil (%0.1 > Olasılık > %0)	D	D	D	O	O

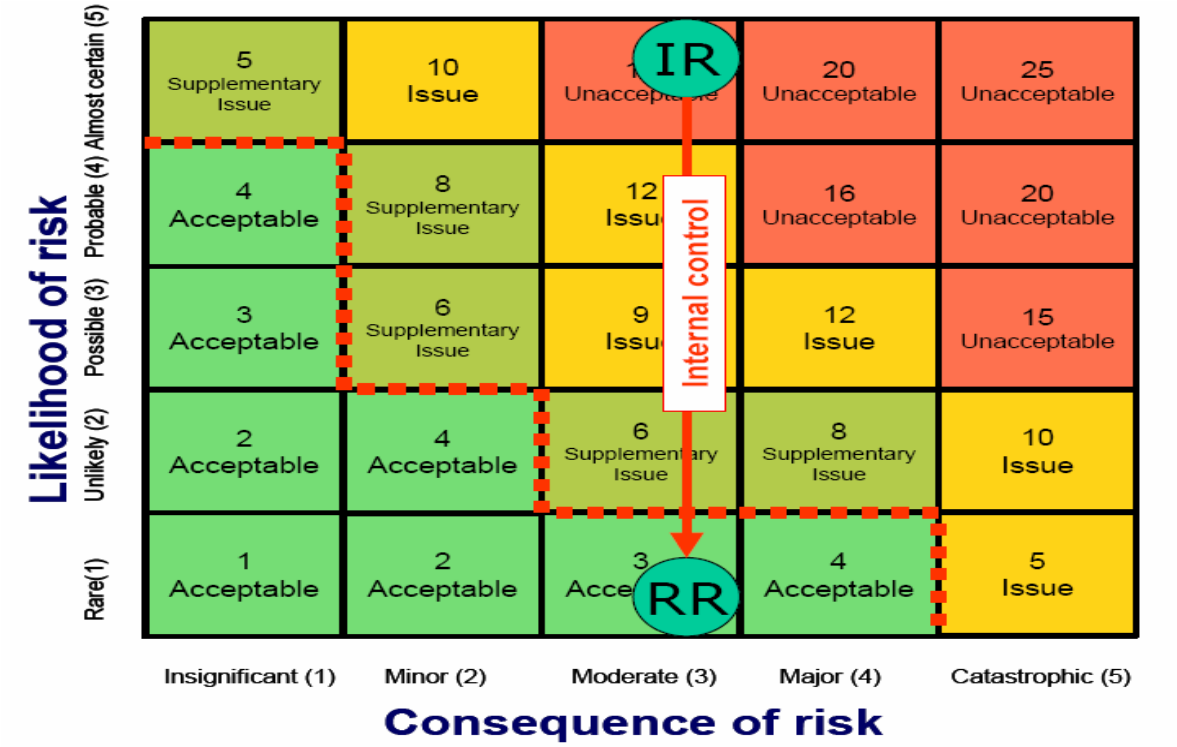
ÇY: ÇOK YÜKSEK	Riski Yönetmek için tedbirler acilen alınmalıdır.
Y: YÜKSEK	Riski Yönetmek için tedbirler alınmalıdır.
O: ORTA	Aksiyon alınması önerilebilir.
D: DÜŞÜK	Aksiyona gerek yoktur.

2.3.7. Adım 7: Kontroller ve Net Risk Düzeyinin Belirlenmesi

Tanımlanan risklerin olasılık ve etki düzeyleri belirlendikten sonra kurumun risk toleransı da dikkate alınarak her bir brüt risk için riskin derecesi bulunmuş olur. Tablo 14'de olasılık ve etki düzeyleri beş derecede belirlenmiş, brüt risk düzeyleri düşük, orta, yüksek ve çok yüksek olarak dört farklı derecede belirlenmiştir.

Bu adımda her bir brüt risk düzeyi için kontrol çevresi değerlendirilip net risk düzeyine ulaşılmaya çalışılır. Sonuçta belli bir riske yönelik uygulanan kontroller o riskin

gerçekleşmesi durumunda varlık üzerinde yaratacağı etkiyi ve riskin gerçekleşme olasılığını azaltmaya yönelik rol oynar.



Şekil 6: Kontrollerin Brüt Risk Düzeyini Net Riske Getirmesi

Kaynak: David Griffiths, **"Risk Based Internal Auditing"**, 15/03/2006, Version:2.0.3, http://www.internalaudit.biz (14 Şubat 2007), s.20.

*__IR:__ Inherent Risk (Brüt Risk), __RR:__ Residual Risk (Net Risk

Şekil 6'da yer alan kırmızı kesik çizgi kurumun risk toleransını belirlemektedir. Bu sınırın içerisinde kalan riskler kabul edilebilir (Acceptable) seviyelerdedir. Bu bölgedeki riskler için fazladan bir kontrol aksiyonu almaya gerek yoktur. Fakat şekilde risk iştah sınırının dışında kalan riskler için kurumun herhangi bir kontrol faaliyeti uygulamaya koyması gereklidir. Burada amaçlanan, alınacak kontroller ile brüt risk(IR:Inherent Risk) düzeyini kabul edilebilir bir net risk seviyesine (RR:Residual Risk) veya daha aşağı bir seviyeye indirmektir[191].

[191] David Griffiths, "Risk Based Internal Auditing", 15/03/2006, Version:2.0.3, http://www.internalaudit.biz/files/implementation/Implementing%20RBIA%20v1.1.pdf (14 Şubat 2007), s.20.

Kontrol çevresi kurumun kontrol bilincidir; çalışanların iş ile ilgili faaliyetlerini yürüttükleri ve kontrol zorunluluklarını karşıladıkları bir çevredir. Kontrol faaliyetleri, riskleri yöneten faaliyetlerin doğru şekilde ve zamanında işlediğinden emin olmaya yarayan politika ve prosedürlerdir. Kontrol faaliyetleri operasyonla iç içe olmalıdır ve riskleri kabul edilebilir düzeylerde yönetmek için kullanılmalıdır. Kontrol faaliyetleri riski önleme, tespit etme ve düzeltmeye odaklıdır. Kontroller sistemsel yani otomatik veya manuel olabileceği gibi kurum seviyesinde, yüksek seviyede veya süreçler ve sistemler üzerinde daha düşük seviyelerde de olabilir[192].

Kurum oluşturacağı risk yönetim modelinde her bir brüt riske uygulanan kontrollerin derecesini belirleyebilir. Örneğin modelde kontrollerin etkinliğini "kontrol yok", "düşük", "orta" ve "güçlü" olarak derecelendirebilir. Kontrol seviyesi ve brüt riskleri karşılaştırarak her bir risk için net risk düzeyine ulaşabilir. Tablo 15'de örnek bir matris yer almaktadır.

Tablo 15: Net Risk Düzeyinin Belirlenmesi Matrisi

NET RİSK DÜZEYİ		BRÜT RİSK DÜZEYİ			
		DÜŞÜK	ORTA	YÜKSEK	ÇOK YÜKSEK
RİSK YÖNETİM SİSTEMLERİ	ZAYIF	D	O	Y	ÇY
	KABUL EDİLEBİLİR	D	D	O	Y
	GÜÇLÜ	D	D	D	O

ÇY: ÇOK YÜKSEK	Riski Yönetmek için tedbirler acilen alınmalıdır.
Y: YÜKSEK	Riski Yönetmek için tedbirler alınmalıdır.
O: ORTA	Aksiyon alınması önerilebilir.
D: DÜŞÜK	Aksiyona gerek yoktur.

Örneğin brüt riski çok yüksek, kontrol etkinliği düşük olan bir risk düzeyinin net riski yüksek çıkarken, brüt riski çok yüksek ama kontrollerin etkinliği güçlü olan bir risk için net risk düzeyi "orta" olabilir.

[192] Naciye Kurtuluş ve Müge Aşlan, **Risk Odaklı İç Denetim Konferansı**, DEVAK Deloitte Academy, 18-19 Haziran 2008, Ritz Carlton, İstanbul.

Bu adım sonunda varlık-tehdit matrisinden yola çıkarak belirlenen her brüt riske uygulanan kontroller neticesinde net risk düzeyine ulaşılmıştır. Böylece kurumun bir risk haritası belirlenmiş olur. Bu adım sonunda elde edilen risk haritası kullanılarak bir risk değerlendirme raporu hazırlanmalıdır.

2.3.8. Adım 8: Aksiyon Alma

Aksiyon alma şeklinde ifade edilen bu adım "Risk İşleme" olarak da isimlendirilmektedir. Teorik olarak, sistemlerin, insanların, süreçlerin veya dışsal faktörlere bağlı unsurların sıfır hata ile yada yüzde yüz güvenilirlik ile çalışması mümkün. olmadığından sistem ve varlıklarla ilişkili riskleri sıfıra indirmek imkansızdır[193].

Bu adımda risk değerlendirme raporunda yer alan riskler için alınacak aksiyona karar verilir. Belli bir risk karşısında "riski kabullenme", "riskin azaltılması", "riskten kaçınma" ve "riskin paylaşımı/transferi" olmak üzere dört farklı aksiyon alınabilir[194].

1. **Riskin Kabullenilmesi:** Bazı riskler, etkileri ve olma olasılıkları düşük olduğundan dolayı ufak sayılır. Bu durumda, riski iş yapmanın bir maliyeti ve bedeli olarak bilinçli bir şekilde kurum politikalarına ve risk kabul ölçütlerine uyması şartıyla riskin objektif bir biçimde ve bilerek kabul edilmesi ve riskin etkisinin düşük düzeyde kalmasını sağlamak amacıyla riski periyodik olarak izlemek uygun olur.
2. **Riskin Azaltılması:** Riskin gerçekleşmesini önlemek veya etkilerini asgari düzeye indirmek amacına yönelik uygun kontroller uygulanarak riskler ortadan kaldırılabilir veya kabul edilebilir seviyelere düşürülebilir.
3. **Riskten Kaçınma:** Bir riskin belirli bir teknolojiyi, tedarikçiyi veya satıcıyı kullanmakla bağlantılı olması olasılığı vardır. Risk, o teknoloji daha sağlam

[193] Shirley Booker ve Diğerleri, "What Is Your Risk Appetite? The Risk-IT Model", **Information Systems Control Journal**, Volume 2 , 2004, http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18439 (12 Kasım 2008), s.2.
[194] GTAG, Global Teknoloji Denetim Kılavuzu, "Bilgi Teknolojisi Kontrolleri", **IIA: Uluslararası İç Denetçiler Enstitüsü**, ,2005, http://www.tide.org.tr/tideweb/resimler/upload/Documents/GTAG, (16 Haziran 2008), s.51-52.

ürünlerle değiştirilmek suretiyle ve daha kalifiye tedarikçiler ve satıcılar aramak suretiyle bertaraf edilebilir.Riskin oluşmasına neden olan faktörleri ortadan kaldırarak riskten kaçınılabilir.

4. **Riskin Paylaşılması/Transfer Edilmesi:** Risk, ticari ortaklar ve tedarikçilerle paylaşılabilir. Bunun iyi bir örneği de, altyapı yönetimi hizmetinin dış kaynaklardan temin edilmesidir. Böyle bir durumda, tedarikçi, IT altyapısının yönetilmesiyle bağlantılı riskleri, asıl kurumdan daha kalifiye ve uzman olması ve daha kalifiye personele erişim imkanına sahip olması sayesinde azaltır. Risk, gerçekleşen risk olayının maliyeti bir sigortacıya aktarılmak suretiyle de azaltılabilir.

Aksiyonlardan hangisinin alınacağına ise fayda/maliyet analizi ile karar verilebilir. Örneğin kurumun net risk düzeyi "çok yüksek" olan bir riski azaltmak ve risk toleransı sınırlarına uygun bir seviyeye indirmek için katlanacağı maliyet, alınacak bu aksiyondan sağlanacak faydadan küçük yani daha az maliyetli ise "riskin azaltılması" yönünde bir aksiyon benimsenebilir. Bu analizde sadece finansal maliyetlere bakılmamalı, ün azalması ve imaj kaybı gibi parasal olmayan faktörler de dikkate alınmalıdır[195].

2.3.9. Adım 9: Artık Risk Onayı

Kontrollerin gözden geçirilip tespit edilen tüm riskler için alınacak aksiyonlar belirlendikten sonra, yine de kalan risklere artık risk (residual risk) denir. Bunlar kabul edilen riskler veya tamamen ortadan kaldırılamayan riskler olabilir. Kurum üst yönetimi, hatta yönetim kurulu artık risklerin kabulü ve aksiyon planının uygulanması için onay vermelidir.

2.3.10. Adım 10: Risk Yönetim Döngüsünün Gözden Geçirilmesi

Üst yönetimce onaylanan aksiyon planının gerektirdiği şekilde hareket edilerek bilgi güvenlik ve risk yönetim süreci uygulanır. Risk yönetim süreci kendisini tekrarlayan ve süreklilik arz eden bir döngüdür. Oluşturulacak uygun kontrol ve kontrol hedefleri ile

[195] GTAG, Global Teknoloji Denetim Kılavuzu, s.82.

kurumun risk değerlendirme raporunda yer alan riskleri, aşağıya kabul edilebilir seviyelere indirilmeye çalışılır. Bilgi işlem ile ilgili olarak TS ISO/IEC 17799:2005 standardında ilgili kontrollerden detaylı bir biçimde bahsedilmektedir. Standartta yer alan kontroller kurumlara rehberlik etmek amacıyla verilmiştir. Sonuçta her kurum belirleyeceği bilgi güvenlik politikası ve risk değerlendirmesi neticesinde bünyesine uygun, kendine özel kontrolleri belirleyebilir.

2.4. Süreç Kaynaklı Operasyonel Riskler ve Yönetimi

Süreçlerin yeniden yapılandırılması ile amaçlanan, operasyonel riskin en önemli nedenlerinden biri olan işlemeyen ya da uygun olmayan süreçlerin daha basit hale getirilmesidir. Bu amaçla süreç içinde elle yapılan işlem ve kontrollerin azaltılması etkin bir yöntem olarak görülmektedir. Böylece hata yapma olasılığı ve işlem hacimlerindeki değişimlere ayak uyduramama riski azaltılmış olurken, tasarruf edilen kaynaklar daha etkin hizmetlerde kullanılabilmektedir. Süreçlerin yeniden yapılandırılmasında kullanılabilecek bir diğer yöntem ise süreçlere ilişkin haritaların oluşturulmasıdır. Süreç haritalarında; faaliyetlere ilişkin tüm süreçler, bunlara ait alt süreçler, söz konusu süreçlerde görev ve sorumluluk sahibi olanlar, yetki sınırları, işlem limitleri, çalışma teknikleri, kullanılacak ürün ve hizmetler vb. unsurlar açıkça belirlenmekte ve bu şekilde süreçlerde yaşanabilecek aksaklıklar nedeniyle ortaya çıkabilecek operasyonel risklere karşı önlem alınmaktadır. Süreçlerin basit, anlaşılır ve herkesçe bilinen yazılı prosedürler haline getirilmesi, kurum içi şeffaflığın artırılması ve üst yönetimin riskleri fark etmesini kolaylaştırması açısından da önemlidir.

2.4.1. Süreç İyileştirme

Bilgisayar ve iletişim teknolojisindeki gelişmeler, kurumların birimleri ya da müşterileri ve tedarikçileri arasında daha önceden var olmamış olan bazı uygulamaların geliştirilmesiyle şirketlerin birbirlerini “okumaya” başlamasını sağlamaktadır ve böylece de kurumlar rekabetçi bir avantaj kazanmaktadırlar. Bilgi teknolojilerindeki değişim ve bu değişimin şirketlerce yoğun bir biçimde kullanılması geleneksel iş yapma tarzını da değiştirmektedir.[196]. Daha basit bir şekilde gerçekleştirilemeyeceği düşünülen bir çok iş,

[196] Hussain, s.125.

temel mantığına bağlı kalınma koşuluyla içeriğinde gerçekleştirilen bazı düzenlemeler sonucunda daha basit bir şekilde yapılabilmekte ve daha az hata oluşabilmektedir. Yeniden düzenlenen iş akışları ve süreç iyileştirmeleri neticesinde iş süreçleri, kullanılan kaynaklar, girdiler ve karar verme süreçleri değişmektedir. Örneğin, EFT işlemlerinin "Real Time Gross Settlement" ile gerçekleştirilmesi neticesinde iki farklı banka müşterisinin karşılıklı ihtiyaçları minimum iş gücü kullanılarak gerçekleştirilmektedir. Her iki bankanın çalışanlarının manuel kontrolü ve desteği gereksiz hale gelmiş olup, oluşabilecek personel kaynaklı riskler ortadan kalkmıştır. Sonuç olarak işlem süresinin kısalması, hataların en aza indirilmesini, iş hacimlerine bağımlılığın ortadan kalkmasını ve daha da önemlisi bankaların ellerindeki personel kaynağını kar marjı daha yüksek olan işlere kaydırabilmesini sağlamaktadır. Operasyonel risk yönetimi açısından anlamı ise oluşabilecek risk potansiyelinin ciddi oranda azalmasıdır, çünkü böylelikle iş sürecine dahil olan girdi sayısı azalmakta, daha şeffaf ve sistemsel olmakta ve çok daha az manuel girdi gerekmektedir.

Süreç iyileştirmesi ISO 9001:2000 kalite standardı içerisinde "Sürekli İyileştirme" bölümü altında yer almaktadır. Sürekli iyileştirme, kalite yönetim sisteminin bir parçası ya da bu sistemde yer alan basit bir proses olarak değil, sistemi yönetme şekli olarak ele alınmıştır. Eğer sonuçlar hedefleri karşılamada yetersiz ise, problem kalite yönetim sistemindedir. Dolayısıyla sistem, kalite hedeflerini başaracak şekilde iyileştirilmelidir. Bu da yönetimin sorumluluğundadır. İşin kolayına kaçılarak problemlerden direk çalışanların sorumlu tutulması kuruma hiç bir yarar sağlamayacaktır. Hedefler başarıldığında, yeni hedefler belirlenmeli ve sistemin bu hedefleri başaracak şekilde nasıl iyileştirilebileceği araştırılmalıdır[197].

Genel olarak iş süreçlerinin iyileştirilmesi, tekrar eden işlemlerin ve kontrollerin sadeleştirilmesiyle, sistemsel olarak gerçekleştirilemeyen ve personelin manuel çabasıyla işleyen süreçlerin ve iş akışlarının azaltılarak otomatik hale getirilmesiyle sağlanır. Süreçleri basitleştirmek ve sadeleştirmek operasyonel risk yönetimini de kolaylaştıracaktır. Çünkü maruz kalınan operasyonel risklerin bir kısmı, karmaşık şekilde gerçekleştirilen işlemlerin ve süreçlerin sonucudur. Örneğin, şube tarafından gerçekleştirilen bir

[197] Türker Baş ve Murat Oymak, **ISO 9001:2000 Kalite Yönetim Sistemi**, 3.Baskı, Ankara:Seçkin Yayıncılık, 2007, s.204-205.

kredilendirme sürecinde müşteri limitlerinin sisteme gömülmesine bağlı olarak şubenin suiniyetine veya şube personelinin dikkatsizliğine bağlı olarak fazladan gerçekleşebilecek olan kredi tahsisi engellenmiş olur. Sistemsel olarak oluşturulan engel, şubece istense bile geçilememekte ve böylece operasyonel risk oluşma potansiyeli azalmaktadır. İş süreçlerini basitleştirilmesi ve iyileştirilmesi kuruma verimlilik ve etkinlik sağladığı gibi, aynı zamanda da şeffaflık sağlayarak raporlamaların etkinliğini artırmaktadır.

İş süreçlerindeki iyileştirmeler esas olarak süreç haritalarını temel alarak gerçekleştirilmektedir. Süreçlerin iyileştirilmesi ve sadeleştirmesi çalışmasından sorumlu olan ekipler hangi işlemlerin ve faaliyetlerin değer yarattığını ve hangilerinin ürettiği değerin görece sınırlı olduğunu tespit etmeye dönük olarak süreç haritalarını ortaya çıkarırlar. Bu haritalar aynı zamanda, iş süreçleri içinde yer alan risk noktalarını tespit etmekte de önemlidir. Bu haritalar temel alınarak, iş süreçleri içinde yer alan işlemsel adımlar gözden geçirilmekte, çalışanların çalışma yerlerinin değiştirilmesi senaryoları kullanılmakta, çalışma yöntemleri ve yaklaşımları sorgulanmakta, işlemleri gerçekleştirmek için kullanılmakta olan teknolojik aletler ve sistemler yenilenmekte ya da üretilen raporlar ve dokümanlar daha anlaşılır şekillere kavuşturulmaktadır. Burada sayılan işlemler gerçekleştirildikten sonra, süreç iyileştirmesinden sorumlu olan ekip ya da danışman firma, personele daha fazla eğitim verilmesi, kontrol noktalarının etkinliğinin artırılması ve sorumlulukların daha net bir şekilde tanımlanmasına dönük tavsiyelerini kuruma bildirmektedir.

Yukarıda süreç iyileştirmenin kuruma operasyonel riskin azaltılması ve verimliliğinin artırılması noktalarında ne türde katkılar sağlayabileceğini anlatıldı. Ama iş süreçlerinin iyileştirilmesi ve sadeleştirilmesine dönük projelerin ne kadarının başlangıçta belirlenen hedeflere ulaştığı da ayrı soru işaretidir[198.]. Hatta, kurumlar anlamlı bir sonuca ulaşmama ihtimaline rağmen süreç iyileştirmesi projesi esnasında zaman zaman gereksiz yere karmaşıklığa ve strese girebilmektedirler. İş süreçlerinin iyileştirilmesi projesini etkisiz ve sonuçsuz bırakabilecek en önemli unsur, üst yönetimin tam desteğine sahip olmamaktır. Net ve kararlı bir şekilde belirlenmiş hedeflerin ve üst yönetimin güçlü desteğinin olmadığı, kurumsal stratejik hedefler ile süreç iyileştirme arasındaki bağlantının

[198] **The Economist,** 1994'den Marshall, s.357.

tesis edilmediği durumlarda başlangıçta hedeflenen sonuçlara ulaşmak zor olacağı gibi boşa emek ve kaynak sarf etme riski de vardır . Üst yönetimin güçlü desteği çok önemlidir, çünkü iş süreçlerinin yeniden yapılandırılması demek çoğunlukla bazı personelin yaptığı işin gereksiz olduğunu ortaya çıkaracak ve personel arasında huzursuzluk doğurabilecektir. Diğer taraftan, iş süreçlerinin iyileştirilmesi sonrasında mevcut işlerini koruyan personel ise daha öncesine kıyasla daha fazla iş gerçekleştirmesine karşı aynı haklara sahip olması karşısında daha farklı bir huzursuzluk içine girebilecektir.

Süreç iyileştirme konusunda bir başka risk noktası otomasyona geçilmesine bağlı olarak ortaya çıkabilecek sorunlardır. Otomasyona geçilmesi sonrasında sistemin çalışmasının ne kadar etkin ve güvenilir olduğu, istisnai olaylar karşısında çalışıp çalışmadığı gibi sorunlar bu kapsamdadır. Çünkü, belirli işlemlerde otomasyona geçerken de ilgili yazılımı kuran da nihayetinde bir insandır ve insanın, dahil olduğu her süreçte doğal olarak hata yapma olasılığı da mevcuttur. Diğer taraftan, süreç iyileştirme ve özellikle otomasyon orta düzeydeki yöneticilerin sahip olduğu kurumsal tecrübeyi bir şekilde göz ardı etme potansiyeli de taşımaktadır. Bunun için, süreç iyileştirme kapsamında geliştirilmiş olan sistemlerde hata ortaya çıktığı zaman personelin, kontrolü eline geçirebileceği, gerekli olan işletimi sağlayabileceği ve problemleri çözebileceği şekilde tasarlanmalıdır. Süreç iyileştirme sadece maliyetleri azaltmak amacıyla gerçekleştiriliyorsa her zaman istenen sonuçları vermeyebilir, hatta bazen riskleri azaltmak, verimliliği artırmak amacıyla gerçekleştirilen projeler bazen risklerin artması ile de sonuçlanabilir. Örneğin, teftiş, denetim veya kontrol görevini yerine getiren ve kar elde etmekten ziyade risklerin yönetimi, kontrolü ve organizasyonel iyileştirmelerin yapılmasını amaçlayan birimlerin görev tanımlarının azaltılması veya ortadan kaldırılmasına dönük süreç iyileştirmeleri bu kapsamda değerlendirilebilir[199].

2.4.2. Politika ve Prosedürleri Oluşturmak

Kurum, operasyonel risk yönetim çerçevesinin temel esaslarını net bir biçimde açıklayan; operasyonel riskin tanımlanması, ölçülmesi, gözlenmesi, kontrol edilmesi gibi süreçleri içeren politika ve prosedürleri yazılı hale getirmeli ve bunlar hakkında ilgili personeli bilgilendirmelidir.

[199] Marshall, s.358-361.

Bu prosedür ve politikalar, stratejik iş planının bütünlüğü içerisinde yer almalı ve temel olarak; risk ölçümlerinin belirli bir düzeyde tutulmasını, risk ölçümüne ilişkin sağlam bir yönergeler ve standartlar bütününü, operasyonel riskin azaltılmasına dönük uygulama talimatları ve kurumun maruz kalabileceği riski ne zaman kabulleneceği, riskten kaçınacağı ya da azaltabileceği bir seviyeye getirmesi gerektiğini tanımlayan kurumsal bir risk algılaması gibi hedefleri gerçekleştirmeyi amaçlamalıdır. Söz konusu politika ve prosedürler operasyonel riskin çerçevesini tanımlamakla beraber aynı zamanda ilgili kişilerin rollerini, sorumluluklarını ve hesap verebilirliklerini de tanımlamayı içermelidir.

2.4.3. Kurumsal Kaynak Planlama

"Enterprise Resource Planning-ERP" (Kurumsal Kaynak Planlama), iş süreçlerinin birbiriyle sistemsel entegrasyonunu sağlayan bir yazılım türü olup öncelikle üretim sektöründe tedarikçiler ve firmanın birimleri arasındaki verilerin transferinden hareketle maliyet etkin bir üretim süreci kurmayı hedefler. ERP, bir şirketin müşterilerini ve tedarikçilerini kurumun üretim sisteminin bir parçası haline getirmenin yanı sıra kurum içindeki birimlerin birbiriyle entegre olabilmesini de sağlar. ERP, kurum tarafından hazine işlemlerinde, mali kontrolde, yatırım yönetiminde, üretim planlamasında, stok yönetiminde, satış yönetiminde, envanter ve makine parkı yönetiminde kullanılmakta olan modüllerin birbiriyle entegre şekilde kendi aralarında konuşmasını sağlar. Her ne kadar ERP modülleri üretim sektöründe yoğun olarak kullanılmakta ise de bazı ERP uygulamaları finansal kesimce rahatlıkla kullanılabilmektedir. Örneğin, muhasebe yönetimini ayrı ayrı şubelerden gerçekleştirmenin ortaya çıkardığı karmaşıklık ve artan operasyonel risk miktarı düşünüldüğü zaman muhasebe yönetimini merkezileştirmek kuruma çok önemli avantajlar sağlayacaktır. Benzer bir biçimde, satın alımların, personel tarafından kullanılan izinlerin ya da belirtilen masrafların merkezi modüller tarafından izlenmesiyle kuruma maliyet avantajları sağlanmış olur.

2.4.4. Toplam Kalite Yönetimi

"Kalite" kelimesi işletme dünyasında üretim ile öncelikli olarak ilişkilendirilmiş olsa da müşteri memnuniyetini ve kurum performansını artırmak için hizmet sektöründe de önemli hale gelmiştir. Toplam Kalite Yönetimi (TKY), müşteri taleplerine her zaman en iyi

şekilde cevap vermeyi sağlamak için belirli kurallar çerçevesinde yönetim süreçlerinin düzenlendiği ve kurumdaki tüm birimlerin dahil olduğu bir üretim sürecidir[200]. Başka bir tanıma göre, TKY verimlilik ve kaliteyi artırmak için bilimsel düşünceye dayanan, hiyerarşik yapısı olmayan ve işleyişi içinde fiyatlandırma bulunmayan bir üretim sürecidir. Bu tanıma göre TKY, bilimsel düşünceye dayalıdır[201]; çünkü kurumun tüm birimlerinde görev alan personelin günlük operasyonel faaliyetleri içersinde bilimsel metotlarla ve aldıkları eğitimlere göre hareket etmeleri gerekmektedir. Hiyerarşik bir yapıda değildir, çünkü karar verme süreçlerini ve inisiyatif noktalarını klasik kurumsal yapılarda olandan farklı bir şekilde üretmektedir. TKY, aynı zamanda transfer fiyatlandırması gibi işleyişi içinde her hangi bir fiyatlandırma içermez. Kısaca, TKY bir kurumda çalışan tüm personelin kalite araştırmasına katılmasını amaçlayan bir felsefe olmakla beraber pratikte de uygulanabilen bir yönetim paketidir ve üç unsuru bulunmaktadır[202]: (i) işe ilişkin olarak mantıksal bir düşünce biçimi geliştirmek, (ii) kaliteyi geliştirmek için çalışanları motive etmek, (iii) pazarlama şansını artırıcı bir şirket kültürü oluşturmak. TKY'nin başarıyla tesis edilebilmesi üst yönetimin liderliğine, kurumun müşteri odaklı yaklaşımına, önce insan anlayışına ve sistematik süreç analizi, denetimi ve sürekli iyileştirmeye bağlıdır. Tüm bu unsurların başarıyla işleyebilmesi de kaliteyi artırmak için çalışanların katkısına, problem çözme ve karar verme tekniklerinin sistematik bir biçimde kullanılmasına dayanmaktadır.

TKY, geleneksel uzmanlaşmaya dayalı olan üretim sisteminin yeniden tanımlanmasıyla üretim hattında görev alan her bir çalışanın otonom olarak kalite denetimini kendisinin ve ondan sonra üretim sisteminde görev alan çalışanın yapmasını amaçlar. Çünkü, klasik üretim sisteminde her bir işçi sadece kendisine tanımlanmış olan görevi yerine getirir ve kalite denetimi ise işi sadece kalite kontrolü olan personellerce gerçekleştirilirdi. TKY yaklaşımıyla, müşteri kavramı iç müşteri ve dış müşteri olarak ikiye ayrılmıştır. Dış müşteri tanımı kurumun ürettiği hizmet veya ürünleri satın alanları açıklarken, iç müşteri tanımı kurumun ürün ve hizmet üretmesinde görev alan her bir

---

[200] P.Capezio ve D. Morehouse, **Taking the Mystery out of TQM,** Career Press, 1995'den Smith, Clifford, **Total Quality Managmenet**, s.61.
[201] K.H Wruck ve M. Jensen, "Science, Specific Knowledge and Total Quality Management", **Journal of Accounting and Economics**, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=55993 (12 Şubat 2008), s.2.
[202] Mehmet Takan, **Bankalarda Toplam Kalite Yönetimi,** TBB Yayın 217, İstanbul, 2000, s.2.

çalışanın kendi aralarındaki görev paylaşımlarına bağlı olarak birbirlerinin müşterisi olmasını ifade eder. Toplam kalite yönetiminin bu yaklaşımı, örgüt içerisinde hiyerarşinin, işbölümü ve bölümlendirmenin kırılması olarak görülmektedir.[203] Yani, üretim hattı üzerinde görev alan her bir çalışan, kendisinden önce dahil olan çalışanın müşterisi konumunda tanımlanmakta ve üretim hattında sonradan gelen "müşteri" de doğal olarak kalite denetimi gerçekleştirmektedir ki bu da yaratıcı rekabeti doğurmaktadır.

TKY sürecinde kullanılan üç adet farklı yaklaşım vardır[204]: Kaizen yaklaşımı, müşteri memnuniyeti, proseslerin etkinliği ve verimliliğinin artırılması için daha iyiyi yapmak, üretmek, sürekli iyileştirmek üzerine odaklanır. Kaizen yaklaşımının iki ana unsuru vardır: koruma ve iyileştirme. Koruma teknoloji, yönetim, işleyişle ilgili mevcut standartların sürdürülmesini anlatırken; iyileştirme ise mevcut standartların iyileştirilmesine yönelik faaliyetleri kapsar. Kalite çemberleri yaklaşımı ise, çalışanların kendi aralarında gruplar oluşturduğu, karşılaştıkları sorunları tespit ettikleri, analiz ve tartışmalarla iyileştirmeye dönük fikirler ürettikleri çalışma gruplarına dayanır. Kalite çemberleri, ufak gruplardan oluşmaktadır ki her bir üye fikrini rahat bir şekilde ifade edebilsin ve çember daha faydalı sonuçlar üretsin. Üçüncü bir yaklaşım ise gerekli ürünleri ve hizmetleri kısa dönemde, gerekli zamanda, gerekli miktarda üretmeyi amaçlayan Tam Zamanında Yönetimdir. Bu yaklaşımın arka planında israfı önleyerek kaliteyi artırmak, verimliliği yükseltmek yatar ve israfı ortadan kaldırmak için de müşterinin aldığı hizmet/ürünlere doğrudan değer eklemeyen tüm faaliyetleri en az düzeye indirmeyi hedefler.

Operasyonel risk yönetimi aslında toplam kalite yönetimi ile birçok ortak paydada buluşmaktadır[205]. Her iki yaklaşımın da temel basamakları arasında fazla fark olmadığı gibi birçok benzer tekniği de kullanabilmektedirler. Risk, kalite gibi süreçlerin sonucunda oluşan çıktılarla ilgilenmektedir. Fakat, risk yönetimi süreçler içinde ve sonucunda oluşan sapmaları ve farklılıkları parasal ifadelerle ilişkilendirmekteyken kalite yönetimi yaklaşımı ise ürün ve hizmetlerin kalitesi yönünden değerlendirmektedir. Çünkü, TKY'nde müşteri ön planda olup bu doğrultuda, hızlı, yerinde ve zamanında hizmet, yenilik, üründe çeşitlilik sunulması, müşteriye yakınlık ve çalışanların motive edilmesi esas alınmaktadır. Toplam

[203] Karou Ishikawa,**What is Total Quality Control: The Japanesse Way**, Londra, Printece Hall, 1985'den Dikmen, M.K. ve Dikmen, A.A, "Her Derde Deva İksir: Toplam Kalite Yönetimi", http://www.tkgm.gov.tr/turkce/dosyalar (07 Temmuz 2008), s.4.
[204] Takan, s.8-11.
[205] Marshall, s.328.

Kalite, karlılığı arttıran bir araç ve müşteri memnuniyetini ön plana çıkartan bir yönetim sistemi olarak işletmelerde yerini almıştır. Daha önceleri firmalar, sadece karlılık ve fiyat rekabeti üzerine çalışmışlardır. Bunlar mevcut yönetim anlayışlarını değiştirerek yerini müşteri isteklerini daha iyi anlayan, müşteri memnuniyetine ağırlık veren ve kaliteli mal ve hizmet sunan kurumlara bırakmıştır. Kalite, maliyetlerin azaltılması veya satışların arttırılması yoluyla ya da her ikisinin birlikte etkisi ile karlılığı arttırabilir.

TKY'nin her bir kurumda uygulanması ve istenen amaçlara ulaşılması da garanti değildir. Kalite yönetimi uygulaması sırasında bazen kurumlar hatalı stratejiler seçebildiği gibi uygulama aşamasında da eksiklikler ortaya çıkabilmektedir[206]. Çünkü, tüm personele yoğun ve kapsamlı bir eğitim vermenin zorluğu ve maliyeti bir kenara, kurumsal yapıda ve iş süreçleri üzerinde ciddi değişimler gerektirebileceği için TKY uygulaması kolay değildir ve uygulama sürecinde standart bir yöntem olmadığı için her bir kurumda izlenecek olan yöntem ve yaklaşımlar farklı olabilmektedir. Ama, uygulama sürecinde ilk yapılması gereken şey, üst yönetimin desteğini sağlamaktır. Çünkü, bir yapıyı değiştirmek ve dönüştürmek amacı doğrultusunda üst yönetimin kararlılığı ve inancı olmaksızın toplam kalite yönetimini uygulamak ve başarı elde etmek mümkün değildir. İkinci adım olarak, toplam kalite konusunda organizasyonda bir 'kalite vizyonu' ve 'kalite felsefesi' oluşturulmalı ve toplam kalite konusunda kurumda üst yönetimde bir "Kalite Konseyi" oluşturulmalıdır. Örneğin ISO 9001:2000'de, üst yönetimin sistem içindeki rolü ve sorumluluklarındaki belirgin düzeydeki artış göze çarpmaktadır. Bu standartta, üst yönetim, müşteri şartlarının belirlenmesi ve karşılanmasının sağlanmasından birinci derecede sorumlu tutulmuştur. Standart müşteri tatmini ile ilgili bilgiyi izlemeyi şart koşmaktadır. Kuruluşun temel amacı müşteri ihtiyaçlarını karşılamak olduğundan, bu bilgi, kalite yönetim sisteminin en önemli performans göstergesidir[207].

Daha sonraki aşamada, kurumda müşteri ihtiyaçlarının belirlenmesi, stratejik kalite planlamasının hazırlanması, kalitenin geliştirileceği alanların tespit edilmesi gereklidir. Toplam kalite konusunda organizasyonda sürekli eğitim son derece önem taşımakta ve en iyi kalite uygulamalarına ilişkin standartların kurum içinde yaygınlaştırılması gerekmektedir. Özellikle operasyonel alanlarda çalışan personel

[206] Wruck ve Jensen, s.3.
[207] Baş ve Oymak, s.13-14.

tarafında, kalite üretiminin önündeki engelleri ortadan kaldırmaya dönük yaklaşımların geliştirilmesi amaçlanmalıdır. Bunun için, çalışan personel risk yönetimi ve kalite yönetimi konusunda gerekli olan kararları ve değişimleri gerçekleştirmesi için motive edilmeli ve yetkilendirilmelidir. Yine bir diğer önemli konu da kurumda performans değerlendirilmesi ve ölçümünün etkin bir şekilde gerçekleştiriliyor olmasıdır, çünkü kalite yönetimi yaklaşımında çalışanların performanslarına bağlı olarak bir ödüllendirme sistemi olmalıdır. Performans ve ödüllendirme sisteminin adil ve etkin olması çalışanların kurum içindeki etkinliğini ve verimliliğini artıracaktır.

2.4.5. Altı Sigma

"Sigma" Yunan alfabesinde bir harftir ve büyük harf sigma (Σ), genellikle toplam'ın simgesini, küçük harf sigma (σ) ise istatistikte bir topluluktaki standart sapmayı tanımlamak, belirtmek için ölçü birimi olarak kullanılır. Standart sapma, istatistiksel olarak bir dağılIm, sapma ve farklılaşma (heterojenlik) ölçüsü olup belirli koşullar altında oluşan değerler arasındaki farklılaşmanın büyüklüğünü gösterir. Söz konusu dağılımda farklılaşma ne kadar büyükse, o dağılımın standart sapması da o denli büyük bir değer olarak hesaplanır. Dağılım içindeki homojenlik düzeyi arttıkça, standart sapmanın değeri azalır. Kalite kontrol sistemlerinin iddialı hedefi de hemen hemen hatasız, sıfır sapmalı sistemlere ve süreçlere sahip olabilmektir[208].

Bu çerçevede Altı Sigma, problemlere ölçülebilir çözüm getirmek, kritik süreçleri optimize etmek ve iş performansı ve karlılıkta belirgin bir iyileşme sağlamak için sorumluluk üstlenilen bir yönetim yaklaşımıdır[209]. Daha genel bir ifade ile ise Altı Sigma programlarının temel amacı kurumsal kültürün dönüştürülerek çalışanların riske ve hata yapmamaya karşı daha duyarlı olmalarını sağlamaktır[210.] Altı Sigma nedir? sorusunu "Altı Sigma Yolu"nun yazarları şu şekilde cevaplar[211]: Kurumsal başarıyı sağlamak, artırmak ve sürekli kılabilmek için kapsamlı ve esnek bir sistemdir. Altı Sigma yöntemi, kapsamlı veri ve

[208] Peter S.Pande, Robert P. Neuman, Roland R. Cacanagh, **The Six Sigma Way, 2000**, Çev. Nafiz Güder ve Güneş Tokcan, **Six Sigma Yolu**, 1.Basım, İstanbul: Klan Yayınları, 2003, s.13.
[209] Gülay Çalışkan, "Altı Sigma ve Toplam Kalite Yönetimi", **Elektronik Sosyal Bilimler Dergisi**, 2006-Yaz, C.5, S.17, s.63.
[210] Hoffman, s.64-65.
[211] Pande&Diğerleri, s.13.

istatistiki çalışmalar ile müşterilerin temel ihtiyaçlarını anlamayı amaçlarken iş süreçlerini yeniden yapılandırmayı, iyileştirmeyi ve yönetmeyi amaçlamaktadır.

Altı Sigma yaklaşımı, yüksek standartlarda üretim yapmayı hedef almış bir kalite yönetim felsefesi olup sigma sayısı arttıkça, kurumun operasyonel faaliyetleri içerisinde hata ve kayıp miktarının azalacağını öngörür. Bu yaklaşım, bir firmanın ürün ve hizmetlerdeki performansını sigma düzeyi ile ölçer ve iş süreçlerinde kayıplara ve hatalara sebep olan nedenleri ortadan kaldırarak kurumun sigma düzeyini sürekli artırır. Bu da iş ve üretim süreçlerinde hataların azalacağı anlamına gelmektedir. Altı Sigma'da hedef, değişkenliği ve sapmayı sıfıra yaklaştıracak, beklentileri mükemmel şekilde karşılayacak ürün ve süreçlere ulaşmaktır.

Altı Sigma metodolojisi, sadece üretim sektöründe faaliyet gösteren kurumlar için değil; aynı zamanda hizmet sektöründe faaliyet gösteren kurumlar için de kullanılabilir bir yaklaşımdır. Finans kuruluşları, sağlık kuruluşları gibi hizmet veren kurumlar da bu metotlardan faydalanarak iş süreçlerini optimize edip performanslarını artırabilirler. Kurumlar, bu yaklaşım ile maliyetlerde azalma, üretkenlikte artış, pazar payında artış, müşteri tatmininde artış, döngü sürecinde azalma, hata oranında azalma hedeflemekte ve olumlu kültürel değişim ile birlikte ürün/hizmet geliştirmeyi amaçlamaktadırlar.

Altı Sigma kısa dönemde kurumsal olarak gerçekleştirilebilecek bir proje değildir ve belirli bir zaman ve bilgi birikimini gerektirmektedir. Altı Sigma yaklaşımının en genel anlamda özetlenebilecek olan dört ana hedefi vardır. Bunlar; müşteri tatminin artırılması, kusurların azaltılması, çıktıların (ürün ya da hizmetler) iyileştirilmesi ve en son olarak da iş veriminin yükseltilmesi ve yeteneğin geliştirilmesidir. Altı Sigma yaklaşımının kurumca etkili ve verimli olabilmesi bazı ön koşulların varlığına bağlıdır. Öncelikle, bu projeyi uygulamak isteyen kurum değişime açık olmalı, farklı ve değişik uygulamaları garipsemeyecek, alışılagelmiş yöntemlerden daha farklı iş yapma tekniklerini kabul edebilecek bir kurumsal kültüre sahip olmalıdır. Değişime ve dönüşüme elverişli bir kurumsal kültürün varlığı tek başına yeterli değildir; zira böyle kapsamlı bir dönüşümü gerçekleştirmek için asıl önemli olan üst yönetimin desteğini almaktır. Üst yönetimin programa liderlik etmesi ve bunu tüm kuruma göstermesi önemlidir.

Altı Sigma sadece bir kalite girişimi olmayıp aynı zamanda kalite yönetimini tamamlayıcı nitelikte bir iş girişimidir. Çünkü, Altı Sigma programı var olan ISO/QS 9000 veya Toplam Kalite Yönetimi sistemi üzerine kurulmalıdır. Altı Sigma var olan kalite programlarının değerlerine zarar vermez fakat tam bir kalite stratejisi için evrimsel bir safhadır. Altı Sigma amacını başarmak için küçük, artan gelişmelerden daha fazlası gerekmektedir. Bu amaç için operasyonun her alanında önemli ve ileri düzeyde gelişmeler olmalıdır.

Altı Sigma organizasyonlarında bütün personele aldıkları eğitimin türüne göre farklı unvan, yetki ve sorumluluk yüklenmekte olup gerçekleştirilen projelerin niteliklerine göre çeşitli çalışma grupları oluşturulmaktadır. Başarılı bir uygulama için projede çalışan ekip görevlilerinin sorumluluk ve görevlerinin tanımlanması gerekir ki bu da Altı Sigma yaklaşımında çalışan görevlilerin çalışma, görev ve sorumlulukları aldıkları kuşak rengine göre sıralanmış ve tanımlanmıştır. İlk bakışta Uzakdoğu sporlarının yapıldığı bir kulübün organizasyon yapısını andıran bu unvanlar, Altı Sigma'nın uygulandığı organizasyon yapısı, uygulamanın kapsamı ve projelerin türüne bağlı olarak çeşitlilik gösterebilir. Şirketlerin büyüklüğü ve uygulamaların kapsamına göre bu görevler birleştirilebilir veya ek görevler oluşturulabilir. Bu yapı sabit değildir ve ihtiyaca göre yenilenebilir bir yapıdır. Ama genel olarak Altı Sigma'nın organizasyon şeması, en yukarıda üst yönetim ve üst yönetim temsilcisini ve hiyerarşik bir biçimde aşağıya doğru kalite şampiyonlarını, uzman kara kuşakları, kara kuşakları ve yeşil kuşakları içermektedir.

Altı Sigma değişim modeli W.Edwards Deming'in PUKO; Planla, Uygula, Kontrol Et ve Önlem Al döngüsüne dayanmakta olup, Altı Sigma yaklaşımında bu model Tanımla, Ölç, Analiz Et, İyileştir ve Kontrol Et, yani (TÖAİK) olarak uygulanmaktadır[212] ve kısaca Tablo 16'da özetlenmiştir.

[212] Pande ve Diğerleri, s.68.

Tablo 16: TÖAİK Altı Sigma İyileştirme Süreçleri Değişim Modeli

	Süreç İyileştirmesi	Süreç Tasarımı/ Yeniden Tasarım
1.TANIMLAMA	✓ Sorun belirleme, ✓ Gereksinimleri tanımlama, ✓ Hedef belirleme	✓ Spesifik yada genel sorunları belirleme, ✓ Hedef belirleme/ Vizyon değiştirme, ✓ Kapsam ve müşteri taleplerini netleştirme
2. ÖLÇME	✓ Sorunu/Süreci doğrulama, ✓ Sorunu/hedefi detaylandırma	✓ Taleplere kıyasla performansı ölçme, ✓ Süreç verimlilik verilerini toplama, ✓ Temel adımları/girdileri ölçme
3.ANALİZ	✓ Nedene ilişkin hipotezler geliştirme, ✓ Birkaç kilit neden tanımlama, ✓ Hipotezleri doğrulama	✓ En iyi uygulamaları saptama, ✓ Süreç tasarımını değerlendirme, • değer katanlar, katmayanlar, • darboğazlar, kopukluklar • alternatif yollar ✓ Gereksinimleri detaylandırma
4.İYİLEŞTİRME	✓ Kök nedenleri ortadan kaldırmak için fikir üretme, ✓ Çözümleri deneme, ✓ Çözümü standartlaştırma, sonuçları ölçme	✓ Yeni süreç tasarlama, • sorun tahminleme, • Yenilikçiliğin uygulanması, • İş akış ilkeleri, ✓ Yeni süreçlerin, yapıların, uygulanması
5.KONTROL	✓ Performansı sürdürülebilmek için standart ölçümlerin geliştirilmesi, ✓ Gerektiğinde sorunların giderilmesi	✓ Performansı sürdürebilmek için ölçüm ve değerlendirmelerin geliştirilmesi, ✓ Gerektiğinde sorunların giderilmesi

Kaynak: Peter S.Pande, Robert P. Neuman, Roland R. Cacanagh, **"The Six Sigma Way, 2000"**, Çev. Nafiz Güder ve Güneş Tokcan, **"Six Sigma Yolu"**, 1.Basım, İstanbul: Klan Yayınları, 2003, s.70.

Tanımlama: Önce şirketin hedefleri ve bu hedeflere ulaşmayı zorlaştıran hatalar tek tek tanımlanır. Tanımlama aşamasında genel ve spesifik sorunlar tanımlanır ve ihtiyaçlar tespit edilir.

Ölçme: Bu aşamada sürecin bütünü içindeki sorunlara yol açan temel adımlar ve girdiler için ölçme teknikleri ve standartları belirlenir. Sürecin verimlilik verileri, hedeflenen düzeyle karşılaştırılır. Ölçmede istatistik yöntemleri kullanılır.

Analiz: Üçüncü aşamada sorunların ve hataların kaynağı ile ilgili hipotezler geliştirilir ve bunlarla ilgili araştırmalar ve doğrulamalar ayrıntılı bir şekilde yürütülür. Analiz sırasında en iyi uygulamalarla karşılaştırma yapılarak süreçteki darboğazların ve kopuklukların bulunması amaçlanır. Hata kaynakları içinde birkaç kilit nedene yoğunlaşmak, zaman ve enerji kaybını önler.

İyileştirme: Hatalara yol açan kritik faktörlerin giderilmesi için üretilen fikirler, bu aşamada değerlendirilir ve en olası çözümler denenir. Gerektiğinde yeni süreçler ve örgütlenmeler geliştirilerek hataların en aza indirilmesi için çalışmalar yapılır.

Kontrol: Son aşamada hataları azaltan performansın sürdürülmesi için standart ölçümler yapılır. Ölçümlerin sonucuna göre sürekli iyileştirme hedefine yönelik çalışmalar sürdürülür.

Kısaca, Altı Sigma anlayışı içerisinde somut verilere dayanılarak sorunların çözümlemeleri yapılmaktadır. Hedefler belirlenir ve süreç bu yönde ilerlemeye başlar. Altı Sigma işletmelerin yaptıkları işlerin başarısını sağlamak ve bu başarıyı artırmak için kullanılan geniş ve esnek bir yapıda olan bir sistemdir ve öncelikli olarak müşteri odaklı hareket etmektedir. Altı Sigma incelendiğinde ortaya çıkan, sadece teknik bir program olmadığı, aynı zamanda da bir yönetim programı olduğudur. Yani bir işletme ve yönetim stratejisidir.

2.4.6. Kurumsal Yönetim İlkelerinin Benimsenmesi

Kurumsal yönetim ilkeleri, şirket faaliyetlerinden doğrudan ya da dolaylı olarak belirli bir fayda sağlayan tüm kesimlerin-sadece sermayedar ya da üst yönetimin değil-çıkarlarını koruyacak şekilde yönetilmesini sağlayan belirli ilkeler bütünüdür. Kurumsal yönetim, aslında girişimcilik, değer üretme, risk yönetimi ve etkin bir gözlemlemeden oluşan ve yönetimin, sermayedarların ve kurumun faaliyetlerinden etkilenen tarafların

çıkarlarını belirli bir dengede tutmayı amaçlayan bir tür kontrol sistemi olarak da tanımlanabilir[213].

Risk yönetimi ile kurumsal yönetim arasında oldukça yakın bir ilişki söz konusudur. Kurumsal yönetim *(Corporate Governance)* kavramı, risk yönetiminin önemine inanan, etik kurallarına bağlı, doğru ve emniyetli bir yönetim anlayışını ifade eden bir kavramdır. Etkin bir şekilde işleyen kurumsal yönetim ilkeleri hem risk yönetiminin etkinliğini artırır hem de şirketin performansında önemli iyileşmeler yaşanmasına katkı sağlar[214].

Risk yönetimi, yönetim kurulu seviyesinde takip edilmelidir. Başka bir deyişle, risk yönetimi her iş biriminin sorumluluğunda olmakla birlikte, izleme görevi yönetim kurulunun sorumluluğunda olmalıdır. Çeşitli iş birimlerinin yöneticileri, iş konuları altındaki fonksiyonlarda mevcut ve olası risklerini tespit etmek ve ölçümlemekle görevli olup, yönetim kuruluna gerekli raporlamayı yapmakla sorumlu olmalıdır. Yönetim kurulu da iç kontrol ve risk yönetimine ilişkin olarak gerçekleştirilen raporlamaları takip etmeli, tüm kurum çapındaki risklerin tespit edilmesi, değerlendirmesi ve yönetimini belirleyen ilkeleri ve yaklaşımlarını belirlemelidir.

Piyasa riskleri, operasyonel riskler ile finansal risklerin doğru ölçümü ve yönetimi ile doğru yönetim tarzı arasında doğrusal bir korelasyon mevcuttur. Çünkü, şirkete yön verecek olan strateji ve politikalar, şirketin piyasa risklerini, finansal risklerini ve operasyonel risklerini ne şekilde yönettiği ile ilgilidir. Bu nedenle, risk yönetimi, proaktif bir yönetim tarzını ifade eder ve şirketin uzun vadeli hedeflerine ulaşmasını ve hissedar değeri *(shareholder value)* dediğimiz değerin, tüm paydaşlara yansımasını sağlar. Risk yönetimi şirketin pazarlama ve finansal faaliyetlerine yansıyacaktır. Böylece, riskini bilen şirket, elindeki mevcut kaynaklarını da doğru tahsis edebilecek ve doğru pazarlama politikaları ile yeni müşterilere ve pazarlara ulaşabilecektir. Risklerini önceden bilen ve tedbir alabilen

[213] Frost, s.287.
[214] Ali Kayım, "Kurumsal Risk Yönetimi ve İç Denetimin Kurumsal Risk Yönetimindeki Yeri", **ActiveFinans**, Ekim-Aralık,2006, s.2.

şirketler proaktif yönetim tarzına sahip şirketler olarak, sonuçlarını da planları doğrultusunda yönetebilmeyi başaran şirketler olacaklardır[215].

Yönetimsel riskler de ölçülebilir hale gelmelidir. Mesleki sorumluluğun belirlenmesi ve yönetimsel zafiyetlerin tespit edilebilmesi neticesinde, şirketler faaliyet gösterdikleri alanlarda kendilerini emniyet altına alabilmektedirler[216]. Mesleki sorumluluk sigortaları ve yönetici sigortaları, dünyada kullanılan sigorta tipleridir. Örneğin halka açılan bir şirketin halka açılma sırasında bir yatırım bankasından danışmanlık hizmeti aldığını düşünelim. Halka açılma sırasında oluşabilecek hata ve ihmal neticesinde oluşabilecek zararların, azınlık hissedarları tarafından dava edilmesi riskine karşı alınabilecek yönetici sorumluluk sigortaları *(Directors and Officers Liability Insurance)* ve herhangi bir yatırım bankasının veya avukatlık bürosunun vereceği danışmanlık faaliyetindeki hata ve ihmal riskine karşı da bir mesleki sorumluluk sigortasının *(Professional Liability Insurance)* olması beklenebilir. Böylece, alınan kararların sorumluluklarına katlanabilme olanağı sağlanmalıdır. Yatırımcıların, yönetimsel kararları sorgulayabilme gücü arttırılabilmeli, kötü yönetim tarzı ayırt edilebilir olmalıdır.

Andersen, Enron, Parmalat, World.com gibi şirketlerin dahil olduğu ve sermaye piyasaları açısından sıkıntılı süreçlerin yaşanmasına bağlı olarak şirketlerin etkin bir iç kontrol, raporlama ve risk yönetim sistemine sahip olup olmadıkları yönünde endişeler oluşmuştur. Çünkü, iş hacimleri devasa olan, finans ile analiz dünyasından yönetim sistemleri ve iş yapma tarzlarına ilişkin olarak övgüler alan çok büyük bir şirketin mali açıdan oldukça sağlam gözüktüğü bir ortamda birden bire yükümlülüklerini yerine getirememesi sermaye piyasalarına, iç kontrol sistemine, dış denetim sektörüne ve yönetim kurullarına olan güveni sarsmıştır. Bu tür skandalların ardından yurt dışı piyasalarda, özellikle Amerika'da yapılan yasal düzenlemeler bu tür sorunları önlemeye dönüktür[217]. Örneğin, çalışmanın ilk bölümünde de ifade edildiği gibi özellikle Sarbanes Oxley Kanunu'nun şirket yöneticilerinin sorumlulukları ve kurumsal yönetim ilkeleri üzerindeki etkisi önemlidir. Çünkü, bu yeni kanun ile, halka açık şirketlerde bağımsız denetim komitelerinin kurulması ve bu komitenin şirketin bağımsız denetimini

[215] Selda Eke, "Risk Yönetimi ve Risk Yönetiminin Kurumsal Yönetim İlkeleri Açısından Önemi" **ActiveFinans**, Mart-Nisan 2005, s.5.
[216] Eke, s.4.
[217] Özkul, s.2-8.

gerçekleştirecek olan şirketin seçiminden ve firma ile olan ilişkilerin yürütülmesinden sorumlu olması ifade edilmiş ve böylelikle de yönetim kurulunun sürece dahil olma olasılığı ortadan kaldırılmıştır. Yine, şirketin mali performansı konusunda üçüncü tarafların lehine şeffaflığı artırmak amaçlı olarak şirketin en tepe yöneticileri kurumun açıklamış olduğu mali tabloların gerçeği yansıttığı konusunda şahsi taahhüt vermeleri zorunlu hale getirilmiştir. Yine, kurumsal yönetim ilkelerin daha iyi çalışmasına ön koşul olarak yönetim kurulunun şirket iç kontrol sisteminin ve mali raporlama sisteminin çalışma etkinliğinden sorumlu olduğu belirtilmiştir[218]. Bu yasadan evvel ABD'de yürürlükte olan mevzuat, şirketlerin kurumsal yönetim uygulamalarının açıklanması yönündeki yaptırımları yeterli görmekte iken, bu yasayla doğrudan kurumsal yönetimin yapılandırılmasına ilişkin hükümler ile daha kapsamlı, detaylı ve cezalandırıcı bir yaklaşım getirilmiştir.

Kurumsal risk yönetimi ve kurumsal yönetim ilkeleri arasında diğer bir ilişki de küreselleşmenin artan şekilde ivme kazanması neticesinde uluslararası doğrudan sermaye ve portföy yatırımlarının artmasıyla yatırımcıların tercihlerinde risk yönetimi ve kurumsal yönetim kavramlarının öne çıkmakta olmasıdır[219]. Çünkü, özellikle gelişmekte olan pazarlarda yatırım yapmak isteyen sermaye, artan bir şekilde kurumsal yönetim ilkelerini uygulayan, şeffaflığı ön planda tutan ve istikrarlı şirketlere yatırım yapmaktadırlar. Yatırımı gerçekleştirecek olan sermayedarlar, fon yöneticileri artık sağlayacakları kazanç dışında, aynı zamanda bu kazancın ne kadar garanti olduğunu da görmek istemektedirler. Bu anlamda da kurumsal yönetim ilkelerinin sıhhatli uygulanması bu konuda en kuvvetli mesajı vermektedir. Çünkü, söz konusu şirket kurumsal yönetim ilkelerine göre yönetiliyorsa, buna bağlı olarak risklerini biliyor, kontrol ediyor, şeffaf bir şekilde yatırımcılar ile paylaşıyor demektir. Dolayısıyla, kurumsal risk yönetiminin tesis edilmesi iyi yönetime dair ilkelerin şirkette uygulanmasının bir parçasını oluşturmaktadır ki bu da şirketin değerini artıran önemli bir etmendir[220].

---

[218] Alan D**.** Morrıon, “Sarbanes Oxley, Corporate Governance and Operational Risk” **Sarbanes-Oxley Seminar**, 22 Temmuz 2004, s.7-13.
[219] ARME soruyor/**ActiveAcademy**, “Risk yönetimi, kurumsal yönetimin bir parçasıdır.” Tamer Saka ile mülakat, s.2-3.
[220] Frost, s.289.

2.4.7. İç Kontrol Ortamının Sağlanması

Basel Komitesi'nce etkin bir biçimde işleyen bir iç kontrol ortamına sahip olmak, performans amaçları yönünden operasyonel verimliliğin ve etkinliğin artırılmasını sağlarken, yönetim raporlaması açısından da finansal ve yönetimsel olarak güvenilir ve eksiksiz bilginin zamanında edinilmesi ile yasalara ve düzenlemelere uygun hareket edilmesini sağlar[221]. Finansal kurumların hızlı bir büyüme sürecine girdiği, pazar payını artırmaya dönük agresif hedeflerin belirlendiği, bilgi işlem sisteminin yenilenmesi ya da yeni bir bankacılık yazılım programının kullanılması yönünde tercihte bulunulduğu, yeni ve karmaşık ürünler sunulmaya başlandığında etkin işleyen bir iç kontrol ve risk yönetimi sistemine sahip olmayan kurumlarda ortaya çıkan riskler daha fazla olacaktır[222].

Bir kurumun iç kontrol sisteminin etkinliği ise, oturmuş bir yönetim ve denetim kültürünün varlığına, kurumun maruz kalabileceği tüm risklerin tanımlanmış olduğu risk setine, verimli ve etkin işleyen kurum içi iletişim ve haberleşme kanallarının varlığına, görev dağılımının ve ayrımının net bir şekilde yazılı olarak uygulamada oluşturulmuş olmasına, operasyonel faaliyetlerin ve işlemlerin periyodik olarak gözlemlendiği bir kontrol ortamının varlığına bağlıdır. İç kontrol sisteminin değerlendirilmesinde üzerinde durulan diğer hususlar ise, üst yönetime operasyonel birimler tarafından güvenilir nitelikte ve zamanında bilgi üretilmesine bağlı olarak, denetim stratejileri oluşturulması, bu stratejilerin uygulanması, kurumun performans, değerlendirme ve karar alma süreçlerinin doğru bir şekilde işletilmesidir.

İç kontrol sisteminin doğru bir şekilde işlemesindeki en önemli faktör, yönetim kalitesidir. Yönetim kurulunun iç kontrol ortamı kapsamındaki sorumlulukları kısaca, risk limitlerinin tesis edilmesi, üst yönetimin performansının ortaya konulması, risk kontrol fonksiyonlarının kurulması olarak belirlenmiştir. Kurumun, müşterilerine veya kendisine belirli hizmet ve ürünleri tedarik eden kurumların risklerine ilişkin olarak geliştirmiş olduğu politika, kurumun iç kontrol kültürü hakkında bilgi verir. Örneğin, şube bir müşteriye limitinden daha fazla miktarda kredi tahsis ettiğinde veya hazine bölümünde çalışan

[221] BCBS, Bank For International Settlements, "Framework For Internal Control Systems in Banking Organization." September 1998, No.40, http://www.bis.org/publ/bcbs40.pdf (14 Eylül 2008).
[222] Ali Kemal Cenk, "Uluslararası Bankacılık Denetim İlkeleri ve Denetim Süreçleri", **Active Finans**, Mart-Nisan 2005, s.2,

personel kendine tanımlanmış olan limitleri aştığında buna karşı her hangi bir önlem alınmıyorsa kurumun iç kontrol ortamının zafiyetinden söz edilebilir. Özellikle finansal kurumlar, risk ve teminat bazlı olarak müşterilerine farklı limitler tesis ederler ve bu limitler dahilinde kredi kullandırırlar. Finansal kurum çalışanları ve birimleri, bu limitlere uymaz ve sistemsel engeller tesis edilemez ise önemli miktarlara varabilecek kayıplar doğabilir. Çünkü, olası bir limit artışı mutlaka ve mutlaka üst yönetimin onayı ve bilgisi dahilinde olması gereken bir işlemdir.

Etkin işleyen bir iç kontrol ortamının tesis edilmesi için personelin kontrollere ve kontrol ortamına ilişkin farkındalığının sağlanması da gereklidir. Çünkü, iç kontrol sisteminin temelinde her personelin gerçekleştirmekte olduğu tüm işlemlerin sonuçlarını öngörebilmesi ve öncelikle kendisinin kontrol etmesi bulunmaktadır. Tüm yetki ve sorumluluk sahibi olan çalışanlar, kurum için eğitimler, uygulama talimatları ve prosedürler ile kurum içi iş akışlarına, işlemlere ve performansa tanımlı ve entegre olan kontrollerin önemini anlamalı ve bu kontrolleri etkin bir şekilde uygulamalıdır. Ayrıca, iç kontrol ortamı belirli bir iç kontrol kültürünün üzerine tesis edilmelidir[223]. Kurum içi kontrol kültürünün oluşturulmasının hem nesnel hem de nesnel olmayan unsurları vardır. Örneğin, böyle bir kültürün kurum içinde oluşturulması için mesleki ve ahlaki standartların geliştirilmesi, tüm personelin iç kontrolün önemini anlaması ve özümsenmesinin sağlanması gerekir. Bunun için de kapsamlı ve sistemli çalışmaların gerçekleştirilmesi, detaylı şekilde uygulama usullerinin oluşturulması, yetki ve sorumlulukların açıkça belirlenmesi, etkin iletişim kanallarının tesis edilmesi gibi unsurların gerçekleştirilmesi gerekir.

Kurumsal iç kontrol ortamı sadece belli başlı prosedürlerin ve uygulama talimatlarının hazırlanması neticesinde tesis edilemez; çünkü bu prosedürlerin işlevsel olabilmesi için gerekli organizasyonel yapıların da oluşturulması ve üst yönetimin de desteği gereklidir[224]. Yöneticiler, iç kontrol ortamının etkin bir şekilde işlemesi gerektiğini önemsediklerini, kararları ve gözlemleriyle göstermelidirler. Yöneticilerin bile iç kontrol ortamının gereklerine uyum sağlamadıkları bir ortamda alt birimlerde çalışan personelin normlara ve kurallara uymasını beklemek boşunadır. Dolayısıyla, etkin bir kontrol ortamının sağlanması için esas koşul üst yönetimin desteğidir.

[223] Yurtsever, s.45-46.
[224] Brink, s.87-89.

İç kontrol sisteminin etkin bir şekilde işleyebilmesi için de kurum içi iletişim kanallarının etkin bir şekilde oluşturulmuş olması ve işlerliğinin sağlanması gereklidir[225]. Kurum içinde bilginin yukarıdan aşağıya, aşağıdan yukarıya ve yatay olarak kurumun tüm yönetim kademeleri ve çalışanlarına ulaşabilecek şekilde akışı sağlanmalıdır. Etkin işleyen iletişim kanallarının varlığı sayesinde, en alt seviyede faaliyet gösteren personel dahi kontrol ve uyarı sürecinin bir parçası olarak gerektiğinde görüşlerini rahat bir şekilde üst yöneticilere aktaracak ve böylece riskli unsurların proaktif bir biçimde yönetilebilmesi sağlanmış olacaktır.

2.4.8. İç ve Dış Kontrol

Denetim denince aklan gelen, çalışanların üst yönetim tarafından çizilmiş sınırlar dahilinde operasyonel faaliyetlerine devam edip etmediklerinin raporlanması ve herhangi bir suiistimal olduğu zamanda gerekli incelemeyi yapıp olayı sonuçlandırmasıdır. Modern finans hizmetleri ve araçları o kadar gelişmiştir ki üst yönetimin düzenli olarak kurumun riskleri ve iç kontrol sisteminin etkin çalışıp çalışmadığı konusunda bilgilendirilmesi gerekmektedir. İç kontrol sisteminin etkin bir şekilde çalışıp çalışmadığı da denetim ekipleri tarafından gerçekleştirilen risk odaklı çalışmalar ile ortaya çıkmaktadır.

İç denetim ekibi, risk yönetimi çerçevesini (stratejisi, süreçleri, altyapısı, çevresi) ve bu çerçevenin nasıl geliştirildiğini ve operasyonlar içerisinde nasıl uygulandığını değerlendirmelidir. Örneğin, kurumun kabullendiği risklerin ya da bazı operasyonel faaliyetlerde riskleri azaltmaya dönük politikaların ne ölçüde genel risk yönetim çerçevesiyle uyumlu olduğu iç denetim ekiplerince incelenebilir. İç denetim aynı zamanda risk yönetiminin etkinliğinin raporlanmasından sorumlu olduğu için, risk yönetim sistemini kurumsal seviyede ele almalı, risk yönetiminin nasıl gerçekleştirildiği ve nasıl raporlandığı konusuna hakim olmalı ve kurumun maruz kaldığı risklere ilişkin olarak mümkün olduğunca tam ve tutarlı bir yaklaşımda olmalıdır. İç denetim ekibi, aynı zamanda periyodik olarak risk ölçümlerini ve risk yönetim sistemlerini gözden geçirmeli ve önemli tutarda ya da olası riskler karşısında üst yönetime bildirimler ve tavsiyeler sunmalıdır[226].

[225] Yurtsever, s.47.
[226] Kevin Down, **Beyond Value At Risk,** Sussex:John Willey&Sons, 1998, s.192.

İç denetim ekiplerinin kurumsal risk yönetiminin etkinliği konusunda üst yönetime görüş verebilmeleri ve kurumsal uygulamalara eleştirel bir gözle yaklaşabilmeleri için öncelikle denetime tabi tuttukları işlerden ve o yöneticilerden bağımsız olmaları gerekmektedir. Bunun için, iç denetim doğrudan doğruya genel müdüre veya mümkün olan durumlarda da doğrudan doğruya yönetim kuruluna raporlama yapmalıdır. Dolayısıyla, kurumsal risk yönetiminin etkinliğinin test edilebilmesi için bağımsız bir iç denetim fonksiyonun olması gerekmektedir. İç kontrolün bağımsız ve etkin olmadığı, kontrol süreçlerinin yetersiz kaldığı organizasyonlarda usulsüz işlemlerin artması beklenmelidir. Böyle bir ihtimale karşı da dış denetim hizmetini sağlayan taraflar, üst yönetim ve/veya yönetim kurulu ile kurumun kredi ilişkisine girdiği taraflar arasında hileli işlemlerin ya da haksız menfaat sağlamaya yönelik eylemlerin var olup olmadığını incelemelidirler ve bu çalışamaya bağlı olarak da görüş belirlemelidirler[227].

Diğer taraftan iç denetim, risk yönetimine ilişkin çalışmaları neticesinde bazı iyileştirme önerileri geliştirdiği gibi operasyonel işleyiş esnasında da bazı öneriler getirebilmekte ya da en azından bazı durumlarda nasıl hareket edilmesi gerektiği konusunda bu ekiplere danışılmaktadır. Bu gibi durumlarda iç denetim ekiplerinin nasıl hareket edilmesi gerektiği yönünde görüş ifade etmemeleri gerektiği, böyle bir davranışın mesleki ilkelere aykırı olduğu yönünde görüşler de vardır[228]. Çünkü, iç denetim ekibinin yanlış bir yönlendirme yapması sonucunda ortaya çıkacak olan sorun yine denetim ekipleri tarafından raporlanacağı için böyle bir durumda çıkar çatışması doğma ihtimali yüksektir. Diğer taraftan da ilgili birim yöneticileri inisiyatif kullanmaları gereken anlarda zaman zaman iç denetim ekiplerinden görüş alarak hareket ederek olumsuz denetim raporlarından kaçınmak istemektedirler. Ama tüm iç denetim ekiplerinin birimlerin maruz kaldıkları riskler ve bu riskleri nasıl azaltabilecekleri konusunda görüş vermemeleri de anlamsız olacaktır. Dolayısıyla, bu tür risklerden kaçınmak ve kuruma artı değer sağlamak için iç denetim ekiplerinin görev tanımlamaları net bir şekilde belirlenmiş olmalıdır ve iç denetim ekiplerinin deneyimli olması sağlanmalıdır.

Günümüzde dış denetimin işleyişinde olduğu gibi iç denetimin işleyişi ve amacı da yavaş yavaş değişmekte ve giderek operasyonel etkinliği ve verimliliği test eden, risk

[227] Cenk, s.9.
[228] Brink, s.103.

yönetimi konusunda yönetime görüş sunan bir yapıya dönüşmektedir[229]. Dış denetim klasik olarak kurumun mali tablosunda açıklamış olduğu kalemlerin gerçekten tam ve doğru olup olmadığının kontrolünün ötesinde kuruma, risk yönetimi, operasyonel etkinlik ile yasal uyum konularında da destek vermektedir. Günümüzde, iç ve dış denetim giderek daha fazla birbirine entegre olma yolundadır, çünkü dış denetim daha makro bir perspektiften bakarak politika ve prosedürleri incelerken iç denetim ise daha detaylı çalışmalar gerçekleştirerek operasyonel etkinliği ve verimliliği inceler. Zaten, Basel Komitesi de iç denetimi gerçekleştiren personel ile dış denetimi gerçekleştirenler arasında iletişimin geliştirilmesi gerektiğini belirtmektedir[230]. Böylelikle, farklı uzmanlık dallarından faydalanılarak, son derece dinamik bir sektör olan bankacılık sektörünün denetiminde yeni çözümler üretmek ve denetim riskini azaltmak mümkün olabilecektir. Bu kapsamda, dış denetçiler, kurumun varlık ve yükümlülüklerinin mali tablolarda açıklandığı gibi olup olmadığı, tutarların doğruluğu ve tamlığı, değerlemelerin güncelliği, gelir üretme potansiyelinin etkinliği ve yasal olarak maruz kalabileceği çeşitli sorunlarla ilgili üçüncü taraflara güvence verir. İç denetçiler, finans sektöründe de giderek daha farklı bir işlevi yerine getirmektedirler. Kurum içi ve kurum dışı mevzuata uyum kontrollerini giderek iç kontrol, yasal uyum ve risk yönetimi birimleri yerine getirirken, denetçiler kurum seviyesinde operasyonel faaliyetlerin bütünlüğünü,verimliliğini ve etkinliğini inceleyip risk yönetimi konusunda görüş vermektedirler. Bu çerçevede, zaman kısıtı ve giderek karmaşıklaşan iş süreçleri karşısında nokta denetimlerin gerçekleştirilmesi, denetime tabi olacak süreç ve birimlerin belirlenmesinde çeşitli ön eleme yöntemlerin geliştirilmesi gerekmekte ve buna bağlı olarak risk bazlı denetim ön plana çıkmaktadır.

Denetçiler tarafından çeşitli iş süreçlerinde ya da birimlerde beklenmedik veya felaketsel risklere ilişkin gerçekleştirilen tespitler daha ön planda incelemeye alınmalıdır. Özellikle bu tespitler, işten ayrılma oranları, personelin formasyon ve tecrübe seviyesi, kullanılmakta olan yazılımların güncel olmaması ya da manuel operasyonel faaliyetlere ilişkinse daha hızlı hareket edilmelidir. Denetim birimlerinin elinde mevcut olan personel de

[229] Haubenstock, s. 259; Marshall, s.399-400
[230] Cenk, s.10.

risk derecelerine göre çalışma alanlarına paylaştırılarak riskler karşısında daha etkin bir gözetim ve kontrol sağlanabilir[231].

2.5. Dışsal Faktörlerden Kaynaklanan Riskler ve Yönetimi

Operasyonel riskler karşısında kurumların daha etkin çalışabilmesi, gerek müşterilerine gerekse de ortak iş yaptığı tüm paydaşlarına karşı her zaman hizmet verebilmesi için operasyonel risk yönetimi kapsamında gerekli olan en önemli araçlardan birisi de her zaman çalışmaya hazır durumda olan hızlı ve temel gereksinimleri karşılayacak şekilde çalışan bir iş sürekliği ve acil durum planının olmasıdır. Bu şekilde bir plana sahip olmak öncelikle üst yönetimin konuya verdiği önem ve desteğe bağlıdır. Üst yönetimden gerekli desteği alan bir planın kapsamlı ve detaylı bir şekilde planlanması, kurumun risk toleransına ve sunduğu hizmetlerin türüne göre değişecek şekilde oluşturulmuş bir acil durum merkezinin kurulması, söz konusu planın periyodik olarak gerçekleştirilecek testlere göre gözden geçirilip güncellenmesi ve acil durum kapsamında kurumun tedarikçilerinin de kendilerinden bekleneni karşılayıp karşılayamadıklarının değerlendirmesi yapılmalıdır. Söz konusu noktalar detaylı olarak aşağıda açıklanmaktadır.

2.5.1. Acil Durum ve İş Süreklilik Planlaması

Acil durum ve iş süreklilik planlarının oluşturulması operasyonel risk yönetiminin ana unsurlarından biridir. Etkin ve işlevsel bir acil durum ve iş süreklilik planıyla gerek kritik faaliyetlerin kısmi olarak kesintiye uğraması gerekse de terör saldırısı, deprem gibi dışsal sebeplerden dolayı faaliyetlerin tamamen durduğu, sistemlerin çalışmadığı zamanlarda bile kurumun kesintisiz faaliyetlerine devam etmesi sağlanarak maruz kalınacak operasyonel risklerden kaçınılmış olunur. Bu çerçevede kurumlar da giderek bu tarz gerçekleşme olasılığı az ama etki seviyesi yüksek riskler karşısında güvende olmak için iş süreklilik ve acil durum planları geliştirmekte ve acil durum merkezlerini[232] hazır hale getirmektedirler. Aksi takdirde, finansal kurumların böyle bir risk karşısında çok önemli boyutlarda kayıplarla karşılaşması kaçınılmazdır.

[231] Marshall, s.399.
[232] Acil durum merkezleri, kurumların faaliyetlerinin yapılan faaliyetin gerçekleştirildiği yerde yapılması imkanı ortadan kalktığında faaliyetin sürdürülebileceği alternatif lokasyonları/merkezleri ifade etmektedir.

Fuji Capital Markets Corporation'ın New York'ta bulunan ofisinin 1993'te World Trade Center'ın bombalanması sonucu faaliyetlerine devam edemez duruma gelmesine, 1.200 kişinin 12 hafta boyunca işten uzak kalmak durumunda olmasına rağmen etkin işleyen bir acil durum planıyla şirket haftanın takip eden ilk iş gününden itibaren tekrar hizmet vermeye başlamıştır[233]. Kurumlar, her zaman Fuji Capital kadar kısa zamanda rutin operasyonel işleyiş durumuna geçememektedir. Özellikle New York, İstanbul[234], Madrid'de gerçekleşmiş olan terörist saldırılar ve yer yüzünün geniş bir coğrafyasında etkili olan kuş gribi salgını sonrasında iş sürekliliğindeki önemli kesintilerden kaynaklanabilecek olan risklerin büyüklüğü konuya verilen önemi artırmıştır[235]. Diğer taraftan, 2004 yılının Ocak ayında Chartered Management Institute tarafından gerçekleştirilmiş olan bir çalışmada enstitüye bağlı olan üyelerden gelen 461 cevaba göre, üyelerin % 25'i BT kapasitesinde kayıp yaşadığını, ama sadece % 1'inin terörist bir eylemden kayba uğradığını belirtmiştir[236]. Çalışma, aynı zamanda cevap veren üyelerin % 53'ünün herhangi bir iş sürekliliği planının olmadığını ve yıllık cirosu 11 milyon sterlinden fazla olan şirketlerin önemli bir bölümünde bu tür acil durum planlarının olduğunu ortaya çıkarmıştır[237].

Felaket, mutlaka bir fırtına, deprem ya da büyük ölçekli bir yangın olmak zorunda değildir. Çünkü kurum içinden ya da kurum dışından kaynaklanan çeşitli sebeplerden dolayı hizmetin durması veya kısmi kesintiye uğraması kesintinin yaratacağı etki boyutuna bağlı olarak "felaket" olarak da tanımlanabilir. Bu yüzden kurumların sahip olduğu veri tabanları, müşteri, tedarikçi ve kredi bilgileri kurumun varlıkları arasında yer alan bina, insan ve ekipmanlar kadar önemli hale gelmiş olup, verilerin korunması ve bilgi sistemlerinin en kısa zamanda ayağa kaldırılması hizmet sürdürülebilirliği için gereklidir.

---

[233] **İç Denetim Dergisi**, "İş Sürekliliği Planlaması" Kış 2003, s.55; Down, s.196.

[234] HSBC genel müdürlük binasının bombalanması sonucunda banka, faaliyetlerine aynı gün içerisinde kısa bir sürede başka bir merkezden (Acil Durum Merkezi) devam edebilmiş, örneğin EFT talimatları kesintisiz yapılabilmiştir.

[235] BCBS, "High-level Principles for Business Continuity" , The Joint Forum, 2005, http://www.cnmv.es/publicaciones/IOSCOPD224.pdf (11 Ağustos 2007), s.5.

[236] Chapman, s.257- 258.

[237] Ayrıca, gelişmiş ülkelerdeki faaliyet gösteren kurumların bile iş sürekliliğine dönük hazır bazı planlarının olmadığı bilinmektedir. Örneğin, ABD' de şirketlerin % 60'dan fazlasının, Avrupa'da 1 milyon Euro dan fazla ciroya sahip kurumların % 90'nın iş sürekliliği planı yoktur. Yine başka bir çalışmaya göre, son 5 yılda önemli bir felaket karşısında iş sürekliliği olmayan firmaların % 93'ü batmıştır. Fortune 500'de yer alan firmaların % 45'i resmi bir iş süreliliği planına sahip,ama bunlardan sadece % 12'si bu planların şirket genelinde etkili olabileceğini düşünüyor. ARME, s.11.

Acil durum planlarının hazırlanmasındaki temel amaçlar müşteriye sunulan hizmetlerde devamlılığın sağlanması, yasal merciler ve üçüncü taraflara karşı olan sorumlulukların zamanında yerine getirilmesi, iş akışlarında karmaşıklığa ve kesintiye sebebiyet vermeden felaketlerin mali etkilerinin azaltılması, felaket anında müşteri ve çalışanların can kayıplarının asgariye indirilmesi ve beklenmedik durumlar karşısında kurumsal varlıkların en iyi şekilde korunmaya alınmasıdır[238]. Ayrıca, acil durum planlaması, gerçekleşmesine ilişkin anlamlı bir tahmin yapılamayan, sektördeki ya da ekonomideki belirli trendlerle ilişkisi olmayan, birlikte iş yapılan ortaklardan, sosyal değişimlerden ve teknolojik gelişmelerden bağımsız olan riskleri dikkate alarak gerçekleştirilmelidir. Örneğin, operasyonları küçültmek ve maliyetleri azaltmak amacıyla bazı fabrikaların ve operasyonların kapatılması sonucu oluşacak çalışanların tepkisi, sendikal tartışmalar, grevler, önemli meblağlar içeren müşteriler veya çalışanlar tarafından açılmış tazminat davaları, patent hakları vb. yönünden kurumun hukuksal sorunlarının oluşması ya da yasa koyucu/düzenleyici tarafından vergi oranlarında ya da belirli harçlarda yapılacak öngörülemeyen artış kurumun operasyonları ve mali rakamlarını etkiler, ama bu kapsamda sayılanlar için acil durum planlaması yanı sıra veya onun yerine kriz yönetimi, yasal savunmalar gibi daha farklı risk yönetim stratejileri de geliştirilmelidir.

Acil duruma konu olan operasyonel riskler, iş sürekliliğini birebir etkileyen, operasyonel faaliyetlerin bağlı olduğu altyapıyı çalışamaz hale getiren ve çoğunlukla kurum dışındaki gelişmelerden kaynaklanan risklerdir. Dolayısıyla, kurum içinden kaynaklanabilecek olan kritik riskler; etkin bir iç kontrol ortamının sağlanması, iş akışları, prosedürler ve uygulama talimatlarının yazılı halde hazırlanmış ve tüm personelin kolayca erişebileceği yerde olması, iç sistem birimlerinin görevlerini etkin ve verimli bir şekilde yerine getirmeleri gibi hususların sağlanması ile yönetilebilir. Mesela, kurumun çok yüksek kritikliğe sahip bilgi işlem sistemleri ya da elektrik, havalandırma sistemi, asansörler, yangın tüpleri gibi diğer varlıkları belirli aralıklarla kalite kontrollerine tabi tutularak kontrol sağlanabilir.

[238] Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, "Bankalar İçin Acil Durum ve İş Süreklilik Planlaması", Türkiye Bankalar Birliği, **Bankacılar Dergisi**, Eylül 2002, Sayı.42, s.20.

2.5.2. İş Sürekliliğinin Sağlanmasında Üst Yönetimin Rolü

İş sürekliliği planlarının hazırlanmasından, değerlendirilmesinden, önceliklerin belirlenmesinden, yönetilmesinden ve gerekli kontrollerin gerçekleştirilmesinden en geniş anlamıyla üst yönetim ve yönetim kurulu sorumludur[239]. Bu kapsamda üst yönetim, etkin ve işlevsel bir iş sürekliliği planın hazırlanmasını, kritik ana iş süreç süreçlerinin belirlenmesini, gerekli mali ve insani kaynakların tahsis edilmesini, planın işleyişinin gözlemlenmesini, gerekirse planda güncelleme ve değişikliklerin yapılmasını ve planının işlerliğinin olmasını sağlamalıdır[240]. Acil durum planının etkinliği ve işlevselliğinden en üst düzeyde yönetim kurulu sorumlu olduğu için, iç denetim ekipleri söz konusu planın üst yönetimin beklentilerini ne ölçüde karşıladığını ve planın kendisini değerlendirmelidirler[241]. Bu kapsamlı inceleme, iş süreçlerine ilişkin gerçekleştirilmiş olan tespitlerin yeterliliğini, olası tehditleri ve geliştirilen senaryoları, iş etki analizlerini, risk değerlendirmelerini, gerçekleştirilen test sonrası tespitleri ve güncellemeleri ve yönetim kuruluna sunulan önerileri içermelidir.

Dolayısıyla, iş sürekliliği planının etkinliği yönetimin desteğine, bu işin tam anlamıyla arkasında olmasına ve gerçekleşen faaliyetlerle ilgili olarak en kritik süreçleri tespit edebilme yeteneğine bağlıdır. Üst yönetimin desteği çok önemlidir, zira acil durum planlarının hazırlanması ve çalışır duruma getirilmesi pahalı olup, uzun, detaylı ve eleman/saat gerektiren bir süreçtir. Hatta bazı kurumlarda üst yönetimin iş sürekliliğinin gerekliliği konusunda ikna edilmesi bile gerekebilmektedir. Çünkü, bazı yöneticiler iş sürekliliğini sadece bilgi işlem sisteminin yedeklenmesi olarak görmekte ve olabildiğince dar kapsamda yorumlamaktadır ve böyle bir plana iş süreçlerinin sahipleri dahil olmadığı için çok zayıf ve eksik bir plan tanımlanmış olmaktadır. Bunun için, acil durum planı hazırlamanın başlı başına bir maliyet olduğu ve özü itibariyle sigorta poliçesi satın almaktan farklı olmadığı yönetim tarafından kavranmalıdır. Çünkü olası bir felaket hiç gerçekleşmeyebilir, ama gerçekleştiği zaman da kurum için hayati önemdeki süreçlerin çalışabiliyor olmasının kuruma kazandıracağı değerler oldukça önemlidir. Acil durum planı hazırlanması maliyetli bir proje olduğu ve bu projenin etkinliği önemli olduğu için sadece

[239] FFIEC, "Business Continuity Planning: IT Examination Handbook", 2003, s.3.
[240] Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, "Bankalar İçin Acil Durum ve İş Süreklilik Planlaması", TBB, **Bankacılar Dergisi**, Eylül 2002, Sayı 42, s.37.
[241] FFIEC, **"**Business Continuity Planning: IT Examination Handbook", 2003, s.21.

kritik olan iş süreçlerinde mevcut kaynaklar kullanılmalıdır. Faaliyetlerin durması sonrası kurumun maruz kalacağı kayıp ve riskler açısından daha az önemde olan süreçler için kapsamlı bir acil durum planı oluşturmak maliyet etkin değildir. Etkin bir plan hazırlanması kapsamlı bir çalışmayı, içerikli bir eğitim uğraşını gerektirdiği gibi zaman zaman kapsamlı ve tutarlı bir şekilde hazırlanmamış olan planların uygulama maliyeti hiç planın olmadığı zamandaki maliyetlerden daha fazla bile olabilir. Çünkü, bilgi sitemlerinde oluşacak olan bir felaket sırasında yanlışlıkla farklı dosyaların yedeklenmesi, daha önceki bilgilerin üzerine yazılması, ya da sadece belli bir kısmı yedeklenecekken tamamının yedeklenmesi gibi daha fazla maddi kayıplara yol açabilir. Bunun için, maliyetler ve sağlanacak olan faydalar dikkatlice gözden geçirilmeli ve yedekleme ile kurtarma aşamasında karşılaşılabilecek olan fazladan riskler konusunda dikkatli olunmalıdır[242].

2.5.3. Acil Durum Planlama Süreci

Acil durum planlarının hazırlanması aşamasında operasyonel faaliyetler arasında en temel ve kritik olan süreçlerin belirlenmesi oldukça önemlidir. Acil durum planı kapsamına dahil edilen kritik iş süreçleri, iş sürekliliğini ciddi bir biçimde etkileyebilecek olan süreçlerdir. Bunun için öncelikli olarak, hangi iş süreçlerinin belirli bir süre faaliyet gösteremeyecek olmasının kuruma maddi ve maddi olmayan sonuçları itibariyle ne kadar zarar verebileceği tespit edilmeye çalışılmalıdır. Örneğin, bir bankanın hazine bölümündeki yazılım ve donanımların zarar görmesi aynı bankanın çeşitli mali raporlamaları gerçekleştirmekte kullanılan yazılımların zarar görmesine oranla çok daha fazla kritiktir. Çünkü hazine işlemlerini gerçekleştiremeyen bir banka kritik parasal işlemleri gerçekleştiremeyeceği gibi ciddi anlamda reputasyon kaybına da uğrayacaktır[243].

Acil durum planlaması kapsamında, öncelikle benzer felaketsel risklere karşı çalışacak olan kriz yönetimi ekipleri oluşturulmalıdır. İş sürekliliği planının geliştirilmesi aşamasında kilit önemdeki personel sürece dahil olmalı ve ilerleyen aşamada da sürekli olarak eğitimlere ve testlere katılmalıdır. Yine iş sürekliliği planı kapsamında faaliyet gösterecek olan diğer personele de gerekli olan tüm eğitim ve dokümantasyon önceden

[242] Marshall, s.408-417.
[243] Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, "Bankalar İçin Acil Durum ve İş Süreklilik Planlaması", Türkiye Bankalar Birliği, **Bankacılar Dergisi**, Eylül 2002, Sayı 42, s.26; ARME, Sayı 5, s.10-14.

sağlanmalıdır. Gerçekleştirilecek olan eğitimler, tüm kuruma yönelik olarak verilebileceği gibi birimlere özel eğitimler de olabilir. Plana dahil olan çalışanlar, ne tür şartlarda planın ne şekilde gerçekleştirileceğini, hangi personelin ne tür bir işlemi gerçekleştireceğini, personel eksikliği olduğu zaman yedeğinin kim olacağını ve o işi nasıl yapması gerektiğini bu eğitimler kapsamında öğrenmelidir. Dolayısıyla, birimler arası gerçekleştirilecek olan eğitimler vasıtasıyla kilit personel eksikliğinde işlerin kesintisiz şekilde yürütülmesi temin edilmiş olacaktır[244].

Acil durum planlamasında ve yönetiminde bir başka önemli nokta da öncü göstergeleri iyi tanımlamak ve onları gözlemlemektir. Çünkü bazı problemlerin önceden tespit edilmesi ve buna bağlı olarak hızlı bir şekilde gerekli aksiyonların alınması oluşabilecek olan felaketlerin büyüklüğünü oldukça azaltabilecektir. Bunun için, süreçler içinde gömülü olan bazı göstergeleri gözlemleyerek ufak olayların daha büyük kayıplara dönüşmesi önlenmiş olabilecektir.

2.5.4. Acil Durum Merkezleri

Öncelikle, kurumsal risk toleransına bağlı olarak ne tür bir acil durum merkezinin tesis edileceğine karar verilmelidir. Zira, acil durum merkezleri taşıdıkları niteliklere göre cold site (kendi ekipmanlarınız ve yedekleme teyplerine ev sahipliği yapacak veri merkezi alanı), warm site ve hot site'lar (operasyona hazır bir veri merkezi) olarak farklı adlar ile anılmaktadır. Eğer tam donanımlı bir acil durum merkezi kurulması planlanıyorsa medya ile temas ve kurum dışındaki taraflarla iletişim sağlanması noktası da dikkate alınmalıdır. Acil durum merkezinde, gerekli olan kritik müşteri bilgileri, ofis ekipmanları, iletişim araçları olmalıdır, çünkü kriz zamanında karşılaşılan en önemli sorunlardan birisi yeterli ve gerekli olan dataların erişilemez durumda olmasıdır. Hatta bazı kurumlar sadece acil durumlarda veri ve bilgi güvenliğini ve varlığını sağlayabilmek için acil durumlarda kullanılmak amaçlı bilgi sistemleri programları kullanmaktadırlar. Bunun için, kurumun binalarında meydana gelecek önemli bir felaket sonrasında elektronik veriler kullanılamayacak duruma gelmesin diye bu tür bilgilerin merkezden uzak bir yerde yedekleniyor olması gerekmektedir. Hatta acil durumlarda çalışanlar tarafından gerçekleştirilmesi gereken en temel fonksiyonlara

[244] FFIEC, "Business Continuity Planning: IT Examination Handbook", 2003, s. 13-14.

ilişkin görev ve işlem tanımlarını anlatan fiziki dokümanlar acil durum merkezinde yer almalıdır.

2.5.5. Acil Durum Planlarının Gözden Geçirilmesi

Acil durum planları belirli aralıklarla gözden geçirilmeli ve belli periyotlarda ya da bazen beklenmedik zamanlarda testleri gerçekleştirilmelidir[245]. Gerçekleştirilen testler neticesinde mevcut planın aksayan yönlerinin olup olmadığı değerlendirilerek gerekli revizyonlar yapılmalıdır. Bu tür simülasyonlarla, oluşabilecek olan felaketin herhangi bir birimdeki ve bölgedeki etkisini görmek mümkün olabileceği gibi kurumsal varlıkların ve çalışanların da nasıl, ne kadar sürede kurtulabileceği simüle edilmiş olacaktır. Acil durum planlarında gerçekleştirilmiş olan revizyonlar ilgili tüm personele iletilmeli ve ekipte görev alanlar her bir adımı gözden geçirip planın ve revizyonların etkinliğini değerlendirmeli ve iyileştirilmesi gereken yada sorun üreten noktaları tartışmalıdırlar[246]. Ayrıca, acil durum planlarının etkin bir şekilde çalışması için en önemli unsur insan kaynağının tecrübesi ve yeteneği olduğu için bu tür planların simülasyon test sürelerinin sıklığı da personelin işten ayrılma oranına göre ayarlanmalıdır.

2.5.6. Acil Durum ve Tedarikçiler

Acil durum ve iş sürekliliği kapsamında değerlendirilmesi gereken diğer önemli bir nokta da kurumun iş ortaklarından aldığı hizmetlerin sürekliliğinin ve performansının sağlanmasıdır. Bu çerçevede, kuruma hizmet sağlayan tedarikçilerin kesintisiz, etkin ve güvenli bir şekilde hizmet sunabilmesi için olaşabilecek riskler gözden geçirilip kabul edilebilir seviyelere indirilmiş olmalıdır. Bu kapsamda, öncelikle kurum dışından tedarik edilen tüm hizmetler, kritiklik seviyesi, önemi ve tedarikçiye göre gruplandırılmış olmalı, her bir tedarikçiye ilişkin olarak rol, sorumluluk, amaç, beklenen hizmetler ve karşı tarafa ilişkin tüm detayları içeren dokümantasyon sağlanmış olmalıdır. İkincil olarak tedarikçilerle olan ilişkileri düzenleyen sözleşmeler, yasal düzenlemeler ve sektörel kaidelere göre belirlenmeli ve gizlilik anlaşmalarını, emanet ve saklama sözleşmelerini, güvenlik ihtiyaçlarının karşılanmasını, alternatif tedarikçileri, olası ceza ve ödülleri de dikkate almalıdır. Ayrıca, kurum, çalışmakta olduğu tedarikçilerin sunduğu hizmetin

[245] Down, s.196.
[246] BCBS, “High-level Principles for Business Continuity” 2005, s.17.

gereksinimlerini karşıladığını, çeşitli sözleşmelerde ve hizmet alım sözleşmelerinde belirtilen şartları yerine getirdiğini ve gösterdiği performansın benzer hizmet sunabilecek olan diğer tedarikçiler ile benzer nitelikte olup olmadığını gözden geçirecek bir iş süreci oluşturulmuş olmalıdır. Diğer taraftan da her bir tedarikçiyle kurumsal ilişkilerin nasıl işlemesi gerektiği yazılı ve resmi bir forma kavuşturulmuş olup kurum ve tedarikçi arasındaki iletişim her iki tarafın isteklerine uygun bir şekilde karşılıklı güven ve şeffaflık çerçevesinde geliştirilmelidir. En son olarak da kuruma mal ve hizmet tedariki sağlayan taraflar ile sözleşmelerin düzenlenmesini, değiştirilmesini ve sonlandırılmasını düzenleyen; özellikle yasal, mali, fikri haklar, güvenlik, rollerin ve sorumlulukların dağılımı vb. açılarından detayları içeren ve hukukçuların da onayı alan bir prosedür mevcut olmalıdır.

Kısaca, etkin ve işlevsel bir acil durum planı hazırlamak için şu hususlara dikkat etmek gereklidir[247]: Hazırlanacak olan acil durum planı birimler, fonksiyonlar bazında değil tüm kurumu kapsayacak şekilde oluşturulmalı, planın ana omurgasını oluşturan iş etki analizleri ve risk değerlendirmeleri özenle gerçekleştirilmeli, planın ne kadar işe yaradığı ve etkinliğinin ancak çeşitli testler gerçekleştirildikten sonra anlaşılabileceği unutulmamalı, test sonuçları ve iyileştirme önerileri bağımsız bir denetim birimi ya da tarafça değerlendirilmeli ve söz konusu plan kurumdaki değişim ve yeniden yapılanmalara paralel olarak gözden geçirilmelidir.

2.6. Operasyonel Risk Yönetimine Dönük Endişeler

Bir çok kurum operasyonel risk yönetiminin etkin ve verimli çalışmasının çok önemli olduğu konusunda hem fikir olsa da, önemli bir kısmı etkin ve sofistike bir risk yönetimini operasyonel faaliyetler içerisinde kapsamlı ve proaktif bir şekilde gerçekleştirmenin oldukça zor olduğunu düşünmektedir.

Çoğu zaman, kurumlar yeni yapılan projelere risk değerlendirmesi yaparak başlasalar da, risk yönetim sürecinin geriye kalan aşamalarını tamamlayamamaktadırlar. Operasyonel risklerin ölçümüne ilişkin en temel sıkıntılar olasılığı düşük ama etki seviyesi çok yüksek olan riskler ile ilgilidir ve bu tür sıkıntıların oluşmasında aşağıda yer alan sebepler belirli ölçüde rol oynamaktadır. Örneğin, bu tür risklere karşı fazla bir aksiyon

[247] FFIEC “Business Continuity Planning: IT Examination Handbook”, 2003, s.22.

alınamayacağına dönük yaklaşımlar, çalışanlar tarafından bu tür risklerin ortaya çıkarılması ve yönetimle paylaşılmasının bazen üst yönetim tarafından olumlu bir şekilde karşılanmayabileceğine dönük yargıların oluşmasına sebep olabilir. Bu tür kalıplaşmış yargıların çalışanlarda oluşmasının sebebi belki de operasyonel risk yönetiminin kuruma kattığı değerin kurum personelince yeterince anlaşılamamış olmasıdır. Yöneticiler, böyle bir yaklaşım tarzıyla da operasyonel risk yönetiminin unsurlarını ve bu çerçevede yapılması gerekenleri tam anlamıyla ve eksiksiz bir şekilde gerçekleştirmek için gerekli olan kaynakları ayırmakta yeterince gönüllü davranmıyor olabilir ya da bütçenin daha sıkı yönetilmesi gerektiği zamanlarda operasyonel risk yönetimi için gerekli olan kaynakları öncelikli olarak kısabilirler. Fakat bunlara rağmen, kurumun faaliyetlerinden doğrudan fayda sağlayan tüm tarafların operasyonel risk yönetiminin kurumsal kültürün önemli bir parçası olduğunu anlaması gereklidir.

Basel II'ye uyum çerçevesinde özellikle finansal kurumların operasyonel risk yönetimi ile ilgili olarak; Basel yükümlülüklerini yerine getirmenin maliyetli olması, yeterli ve esnek bir veri setine sektörün genel olarak sahip olmaması, yetkili düzenleyici ve denetleyicilerin finansal kurumların geliştirmiş oldukları yöntemleri nasıl denetleyip onay verebilecekleri, kamuoyunu bilgilendirmeye dönük artan talepler gibi bazı endişeleri mevcuttur[248].

[248] Akkizidis ve Bouchereau, http://www.ffiec.gov/ffiecinfobase/booklets, (19 Ocak 2007), s.76-80.

2.7. Risk Yönetim Endeksi

Latin Amerika ve Karayipler'de yer alan ülkelerin doğal afetler karşısındaki politika ve uygulama kapasitelerini ölçmek amaçlı olarak söz konusu ülkelerin risk yönetimi performanslarını ve bunların etkinliğini ölçerek bir Risk Yönetim Endeksi (RYE) *Carreno ve diğerleri* tarafından gerçekleştirilen çalışmada[249] oluşturulmuştur. Doğal bir afet sonrasında, çeşitli göstergeler kullanarak risk yönetimini kavramsal, bilimsel, teknik ve sayısal açıdan ölçmenin zorluğundan hareketle ilgili idarenin risk yönetim performansının ölçülmesinde kullanılacak olan göstergelerin net, sağlam, açıklayıcı ve politikacılar açısından da anlaşılır olması gerektiği vurgulanmaktadır. Ayrıca, söz konusu performans ölçümü düzenli olarak uygulanacağı için değerlendirme metodolojisinin kolay uygulanır olması ve dolayısıyla gelişim sürecinin izlenebilir olması gerektiği ve farklı coğrafi bölgeler, şehirler ve ülkeler arası karşılaştırmaya olanak vermesinin gerekliliği ifade edilmektedir[250].

Carreno da yukarıda bahsedilen çalışmasında oluşturmak istediği RYE belirli bir ilerleme düzeyini ifade edecek şekilde ya da mevcut durumun belirli bir seviyeden ya da örnek bir ülkeden ne kadar farklılık gösterdiğinin belirlenmesine yardımcı olması amacıyla tasarlanmıştır. Bu kapsamda RYE, her birinin içinde altı adet gösterge olan dört ana kamu politikasının sayısal ifadelere dönüştürülmesiyle oluşturulmuştur.

Risk Değerlendirme Endeksi (Risk Identification Index-RMI_{RI}): Bireysel algıların bir ölçümü, bu algıların bir bütün olarak toplum tarafından nasıl anlaşıldığı ve nesnel bir şekilde risk değerlendirmesidir.

Riski Azaltma Endeksi (Risk Reduction Index- RMI_{RR}): Riski azaltma ve riske karşı aksiyon alma seviyelerinin ölçülmesidir.

Doğal Felaket Yönetim Endeksi (Disaster Management Index- RMI_{DM}): Alınan aksiyonlar, gerçekleşen iyileşme ve tüm sürecin nasıl yönetildiğine ilişkin çeşitli ölçütleri içermektedir.

---

[249] M.L. Carreño, O.D. Cardona, ve A.H. Barbat, "Evaluation of the Risk Management Performance", 250th Anniversary Of The 1755 Lisbon Earthquake, 2005. http://www.unisdr.org/HFdialogue/download/tp1-Evaluation-risk-management-performance-m1.pdf (6 Şubat 2009).

[250] Carreño ve Diğerleri, s.1.

Mali Koruma Endeksi (Financial Protection Index- RMI_{FP}): Risk transferi ve kurumsallaşma seviyesini ölçmektedir. Risk Yönetim Endeksi (RYI)'de tüm bu alt parçaların ortalaması olarak tanımlanmaktadır.

$$RMI=(RMI_{RI} + RMI_{RR} + RMI_{DM} + RMI_{FP}) / 4 \qquad (4)$$

Doğal afetlere karşı hazırlıklı olmak amacıyla oluşturulacak olan RYI ölçülmesi için dört ana politika alanı oluşturulmuş olup her bir ana politika alanı altında ise altı adet gösterge/alt faktör belirlenmiştir. Bu göstergelerin hepsi ilgili ülke, bölge veya şehrin göstermiş olduğu risk yönetimi performansını ortaya çıkarmaktadır. Daha fazla sayıda alt gösterge kullanımı ağırlıklandırmayı zorlaştıracağı için 6'dan daha fazla alt gösterge kullanılmamıştır. Carreño'nun risk yönetimi metodolojisine göre performans değerlendirmesi gerçekleştirildikten sonra, her bir göstergenin değeri 1=düşük, 5=optimum olacak şekilde beş gösterge seviyesi arasından belirlenmiştir. Böyle bir metodoloji her bir seviyenin eşzamanlı olarak bir "performans hedefi" olarak kullanılmasını ve karşılaştırma ve değerlendirme yapabilme olanağı sağlamaktadır.

Her bir faktör grubuyla ilgili olarak risk yönetimi olgunluk seviyesini gösteren alt indeksler ise aşağıdaki denklem ile elde edilmiştir.

$$RMI^{t}_{c(RI,RR,DM,FP)} = \frac{\sum_{i=1}^{N} w_i I^{t}_{ic}}{\sum_{i=1}^{N} w_i}\Bigg|_{(RI,RR,DM,FP)} \qquad (5)$$

Denklemde w_i her bir göstergenin ağırlığını, I^t_{ic} her bir göstergeye ilişkin ***c*** faktör grubundaki ve ***t*** zamanındaki – normalleştirilerek ya da ifadesel bağlantıdan arındırılarak, (sayısallaştırılarak)- durumu ifade etmektedir. Bunlar her bir faktör grubuna ilişkin risk yönetimi endeksini göstermektedir. Cardona ve Carreño'ya göre bu şekildeki değerleme içeren ifadeler, aşağıdaki denklemlerde parametrik olarak verilen sigmodial ya da bell tipinde bir fonksiyona sahip fuzzy set ile aynıdır (Bkz. Şekil 7).

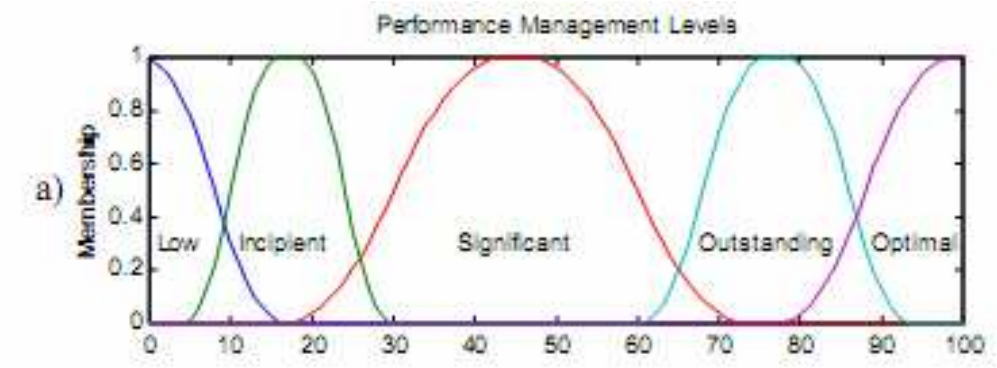
$$bell(x;a,b,c) = \frac{1}{1+\left|\frac{x-c}{a}\right|^{2b}} \qquad \textbf{(6)}$$

b değeri genellikle pozitiftir,

$$sigmoidal(x;a,c) = \frac{1}{1+\exp[-a(x-c)]} \qquad \textbf{(7)}$$

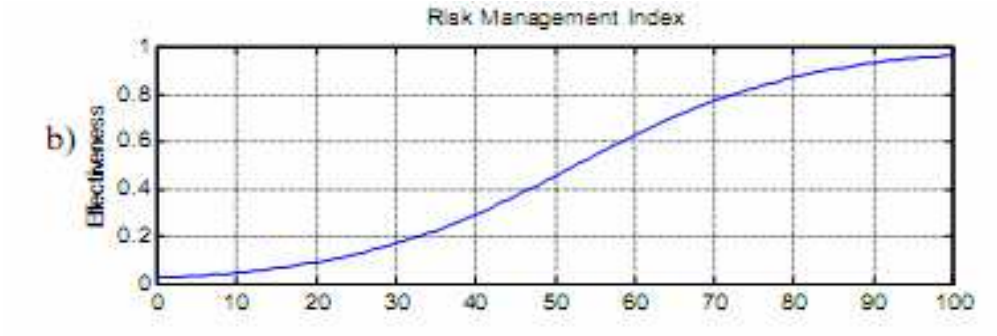
a değeri çakışan noktaların eğimini göstermekte olup 0.5 değerinde *x*=*c* olmaktadır.

Şekil 7: Performans Yönetim Seviyeleri



Kaynak: M. L. Carreño, O. D. Cardona, ve A. H. Barbat, "**Evaluation of the Risk Management Performance**", 250th Anniversary Of The 1755 Lisbon Earthquake, 2005.

Şekil 8: Risk Yönetim Endeksi



Kaynak: M. L. Carreño, O. D. Cardona, ve A. H. Barbat, "**Evaluation of the Risk Management Performance**", 250th Anniversary Of The 1755 Lisbon Earthquake, 2005.

Çalışmada RYE kapsamındaki performans seviyeleri; *düşük - low* -(mevcut riskler karşısında risk yönetimi oldukça zayıf, hatta neredeyse her hangi bir risk yönetimi faaliyeti yok), *başlangıç seviyesinde-incipient*- (yetersiz olmasına karşın belirli bir gayret mevcut), *yeterli derecede -significant*-(risk yönetimi yeterli olmasına karşın, bazı kısıtlar mevcut), *oldukça ileri düzeyde-outstanding*- (iyi yönetilmekte, risk yönetimi konusunda yaratıcı) ve en son olarak da *optimum seviyede-optimal*- (kendi kendini güncelleyebilen, yaratıcı, eş zamanlı çalışan bir risk yönetimi sistemi) şeklinde belirlenmiştir.

Çalışmada, risk yönetiminin etkinliği olgunluk seviyesinin/performans seviyesinin bir fonksiyonu olarak ifade edilmiş ve risk yönetim süreci karmaşık bir süreç olduğu ve artan operasyonel risk yönetiminin *non lineer* özellik gösterdiği

Şekil 8'de gösterilmektedir. Carreno'ya göre risk yönetimi olgunluk seviyesi başlangıçta yavaş olmasına karşın risk yönetiminin iyileştirilmesine ve etkinliğinin artırılmasına dönük olgunluk modeli kapsamında belirtilen iyileştirmeler yapılması ve bu iyileştirmelerde belirgin bir süreklilik sağlanmasına bağlı olarak operasyonel risk yönetimi performansı ve etkinlik düzeyi artmaktadır. Risk yönetimi performansının belirgin bir yüksek seviyeye ulaşmasından sonra gerçekleştirilen iyileştirmeye dönük çalışmalar ise etkinlik seviyesini giderek azalan derecede arttırmaktadır ve marjinal etkisi daha sınırlı olmaktadır. Diğer taraftan risk yönetimi olgunluk seviyesinin çok düşük olduğu durumlarda gerçekleştirilen iyileştirme çalışmaları genellikle istikrarlı bir biçimde işletilmediği için etkinlik ve performansa katkısı da düşük seviyede oluşmaktadır.

Risk yönetiminin nasıl olması gerektiği konusunda tecrübe ve bilgi sahibi olan ilgili uzmanlar faktörleri oluşturan her bir göstergesinin üzerinden geçerek faktör içerisindeki önem ağırlığını belirlemişlerdir. Uzmanlar tarafından belirlenen karşılıklı önemlilik ağırlıkları da Analitik Hiyerarşi Süreci (AHS) kullanılarak incelenmiştir.

Her bir faktör grubunun altında yer alan göstergelerin toplamı 1 olacak şekilde aşağıdaki şekilde hesaplanmaktadır:

$$\sum_{j=1}^{N} w_j = 1 \qquad \textbf{(8)}$$

Yukarıdaki ifadede N her bir faktör grubu altında yer alan gösterge sayısını ifade etmekte olup her bir faktör grubunun olgunluk seviyesi de grup altında belirtilen göstergelere göre kurumun olgunluk seviyelerinin ağırlıklandırılmış toplamıdır ve aşağıdaki formül kullanılarak hesaplanmaktadır.

$$\mu_{RMIp}=\max(w_1 x \mu_c(C_1),....,w_N x\ \mu_c(C_N)) \qquad \textbf{(9)}$$

Formülde geçen w_i her bir faktör grubu içersinde yer alan göstergelerin faktör toplamı içersindeki ağırlığını göstermekte; $\mu_C\ (C_N)$ ise kurumun her bir göstergeye ilişkin olarak mevcut olgunluk seviyesini göstermektedir.

$$RMI_p=[\max(w_1 x \mu_c(C_1),....,w_N x\ \mu_c(C_N))]_{centroid} \qquad \textbf{(10)}$$

ÜÇÜNCÜ BÖLÜM

3. BANKALAR İÇİN OPERASYONEL RİSK YÖNETİMİ OLGUNLUK SEVİYESİ (ORYOS) ENDEKSİ HESAPLANMASI ÜZERİNE BİR MODEL ÖNERİSİ

3.1. Anketin Yapısı ve Olgunluk Seviye Modeli

Bankaların operasyonel risk yönetimi seviyelerini kolay, anlaşılır aynı zamanda da kapsayıcı bir bakış açısıyla ölçerek, karşılıklı değerlendirmeye ve çeşitli kriterlere göre banka gruplarını karşılaştırmaya olanak verecek bir ölçüm yaklaşımı olarak çalışmada "*Capability Mature Model*"-CMM- (Olgunluk Modeli) kullanılmıştır. Böylelikle, alt başlıklara ayrılmış olan ana faktörler içerisindeki her bir alt faktöre ilişkin olarak kurumun mevcut uygulamaları ve durumu *0 (sıfır)-yok* ile *5 (beş)-optimum* arasında olacak şekilde tespit edilmektedir. Kurum, bu ölçek içinde nerede durduğunu, hangi seviyeye erişmeyi amaçladığını ve o seviyeye erişmek için hangi tür uygulamaları geliştirmesi gerektiğini görebilmekte ve bir şekilde kurum için yol haritası çizebilmektedir.

Çalışmada kullanılan, olgunluk modeli konusundaki çalışmalar Philip Crosby'nin araştırmalarına kadar izlenebilmektedir[251]. Onun kalite yönetim sistemi kapsamındaki değerlendirmelerinde kalite yönetim süreci 5 faza bölünmüş olup "*Uncertainty, Awakening, Enlightenment, Wisdom, and Certainty*"den oluşmaktadır. Crosby'nin "evrimsel süreç" yaklaşımı karmaşık yazılımların geliştirilmesi sürecine de uygulanarak Software Engineering Institute (SEI) tarafından 2002 yılında "Capability Maturity Model" oluşturulmuştur[252]. CMM'in oluşturmasının asıl amacı bir kurumun işleyen süreçlerinin iyileştirilmesi ve ürün geliştirme, temin etme ve bakım aşamalarını en iyi şekilde yönetebilmesi için bir rehber sunmaktır. Bu rehberde yer alan genel kabul görmüş yaklaşımlar, kuruma kendi kurumsal olgunluk seviyesini gözden geçirerek hangi noktalarda iyileştirmelerin gerçekleştirilebileceği ve bu iyeleştirmelerin nasıl sonuçlandırılabileceği

[251] Connell, s.8.

[252] CMMI modeli 1986 yılında Amerikan Savunma Bakanlığı'nın (Department of Defense, DoD) isteği doğrultusunda Carnegie Mellon Üniversitesi'ne bağlı Yazılım Mühendisliği Enstitüsü (SEI) tarafından geliştirilmeye başlanmıştır. İlk olarak yalnızca yazılım üzerine, SW-CMM olarak 1991 yılında yayınlanan model, 2002 yılında sektör bağımsız bir şekil alarak "CMMI" olmuş, 2006 yılında ise v1.2 olan son sürümüne ulaşmıştır. **Bütünleşik Yetenek Olgunluk Modeli**, TBD-Kamu-BİB 1. Çalışma Grubu, s.6, 2008

konusunda yardımcı olmaktır. SEI, olgunluk modellemesini 5 süreç üzerinde oluşturulmuştur. SEI'nin modellemesi Tablo 17'de açıklanmıştır.

Tablo 17: Olgunluk Seviyeleri

(1)Başlangıç	Süreçlerin nasıl işlediği tam olarak bilinemiyor.
(2)Yönetiliyor	Süreçler önceden planlanmış bir şekilde işletilmekte. ölçülmekte ve kontrol edilebilmektedir.
(3)Tanımlanmış	Süreçlerin nasıl işleyeceği iyice anlaşılmış olup prosedürlerde, standartlarda, kullanılan araçlarda ve yöntemlerde tanımlanmıştır.
(4)Sayısal olarak yönetilmekte	Süreçlerin performansı ve kaliteli işleyişi statiksel olarak ölçülebildiği ve tüm süreç boyunca yönetilebildiği için her "tahmin edilebilir" durumdadır.
(5)Optimum durumda	Süreçler içersinde bulunan her türlü değişimlere yol açan her türlü sebep sayısal olarak izlenebilmekte ve anlaşılmakta olup sürekli iyileştirmeye girdi sağlamaktadır.

Kaynak: Mc Connell Patrick, "**Measuring Operational Risk Management Systems under Basel 2**", s.8.

Yazılım sektöründeki herhangi bir firmanın olgunluk seviyesine bakarak o firmanın hedeflerini ne şekilde ve nasıl gerçekleştirilebileceği tahmin edilebilir[253]. Olgunluk seviyesinin en alt basamağında değerlendirilen bir firmanın maliyetleri, projenin zamanında teslimi, işlevselliğinin yeterliliği ve sunulan ürünün kalitesi konusunda çok fazla değişiklik görülebilir. Olgunluk seviyesi üzerinde ilerlemek en genel anlamıyla kurumlara tahmin edilebilirlik, kontroller ve etkinlik konularında önemli katkı ve iyileştirmeler sağlamaktadır. Kurumun olgunluk seviyesi ilerledikçe hedeflenen sonuçlar ile gerçekleşen sonuçlar arasındaki fark giderek azalır. Örneğin düşük olgunluk seviyesinde olan firma teslim etmesi gereken bir projeyi önceden anlaşılmış olan tarihten epey farklı bir tarihte teslim edebilir. Diğer taraftan ise daha yüksek olgunluk seviyelerinde olan kurumların ürün proje teslimleri giderek daha belirgin bir şekilde tam zamanında gerçekleşmeye başlar. Ayrıca, kurumun olgunluk seviyesi üzerinde daha ileri aşamalarda bulunması, kontrollerin daha etkin olmasını sağlayarak kurumun genel olarak etkinlik seviyesini de yükseltir. Böylece, olgunluk seviyesi daha yüksek olan kurumların maliyetleri azalır, iş-ürün geliştirme süreci kısalır, verimlilik ve sunulan hizmetteki kalite artar.

[253] Mark C Paulk, Charles V Weber ve Mary Beth Chrisis, "**The Capability Maturity Model for Software**" http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr24.93.pdf (19 Mart 2009), s.10.

Kısaca 1-5 arasında yer alan bu evrimsel süreçte kurum, en alt seviyede karşılaşılan problem veya sürecin nasıl işlemesi gerektiği konusunda çok az bilgiye sahip olunması, uygulama düzeyinin ve farkındalığın zayıf olmasıyla en ileri seviyede söz konusu sürecin diğer iş süreçleriyle entegre bir şekilde çalışarak tüm iş süreçlerinin karşılıklı olarak ayrılmaz bir parçaya dönüşmesi arasında yer almaktadır. Olgunluk modelleri kullanmanın önemli yararları; kuruma, aynı süreçleri farklı durumlarda uygulamasına ilişkin karşılaştırma olanağı veren bir ölçek sunması; herhangi bir süreç içerisinde kurumun profili hakkında bilgi vermesi; kurumun mevcut durumunu GAP analiziyle göstererek hedeflediği seviyeleri belirlemesine ve o seviyeye ulaşması için neler yapması gerektiği konusunda yol göstermesi sayılabilir[254]

COBIT metodolojisi de kurumların BT iş süreçlerindeki kontrol seviyelerini değerlendirirken SEI'nin Olgunluk Modeli'ne benzer bir yaklaşımla COBIT Maturity Model kullanmaktadır[255] Diğer bir ifadeyle, COBIT kapsamında kullanılan Maturity Model SEI'inin geliştirmiş olduğu ve yukarıda genel hatlarıyla açıklanan "Capability Maturity Model" esas alınarak geliştirilmiştir. Her ne kadar COBIT uygulamasında kullanılan olgunluk CMM'den esinlenmiş olsa da önemli birkaç farklılık içermektedir.

CMM yazılım mühendisliği temel ilkeleri kapsamında yazılım ürünleri geliştiren firmaların bu alanda faaliyetlerini ve çalışmalarının mükemmelleştirilmesi ve mevcut olgunluk durumlarının sertifikalanması amacıyla geliştirilmiş olsa da COBIT kapsamında değerlendirilen olgunluk seviyeleri, bir kurumun bilgi teknolojileri yönetim süreçlerindeki olgunluk seviyesi üzerinde durmakta olup genel hatları belirlenmiş ve jenerik olarak

[254] Connell,s.9'den J.W. Lainhart, (2001) "COBIT Management Guidelines IT Governance Forum Trust and Understanding for the Business and the Board", ITGI Paris.
[255] Erik Guldentops, Wim Van Grembergen ve De Haes Steven, "Control and Governance Maturity Survey: Establishing a Reference Benchmark and a Self-assessment Tool", **Information Systems Control Journal**, Volume 6, (2002),.
http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16122&TEMPLATE=/ContentManagement/ContentDisplay.cfm (15 Ocak 2009).

kullanılacak bir olgunluk seviyesini ifade eder.[256]. Bu jenerik modellerden hareketle de 34 adet kontrol hedefi için alt olgunluk seviyeleri belirlenmiştir[257].

COBIT kapsamında oluşturulan olgunluk seviyeleri incelendiğinde her bir seviye için aşağıdaki cümleler ifade edilebilir:

0-Varolmayan (Non-existent): Bir süreç ya da, yerine getirilmesi gereken bir iş akışına gerek bile olmadığı düşünülen; tamamıyla var olmayan bir durumu ifade etmek için bu seviye gösterge olarak kullanılmaktadır. Sürecin varlığı ve işlerliği konusunda bir ihtiyaç olduğuna dair her hangi bir kanıt, işaret, bilinç artışı, sorgulama ve/veya ihtiyaca ilişkin hiç bir eylem olmadığı, sürece ilişkin herhangi bir işin veya alt kontrolün gerçekleştirilmediği gözlemlenmiştir.

1- Başlangıç / Kişiye Göre (Initial/Ad Hoc): Kurumun belli bir konuda bir şeyler yapması gerektiğini belirten, belli bir sorunu çözmesi veya bir işi yapması ile ilgili olarak gereksinim içerisinde olduğuna dair kanıtların olduğu aşamadır. Ancak; standartlara dayalı bir süreç yerine, durumdan duruma değişkenlik gösteren, kişiden kişiye farklı olan plansız ve anlık yaklaşımlar ile iş gerçekleşir. Sorun çözümü ve işleyiş açısından seyrek, tutarsız, düzensiz, kurumun kısıtlı alan ve yönetimlerine yönelik iletişim kurulduğu ve yönetimin kaotik bir yaklaşım içerisinde olduğu bir seviyeyi gösterir.

2- Tekrarlanabilir ancak Sezgisel (Repeatable but intuative): Çözümlenmesi gereken sorunlara ve yapılması gereken işlere ilişkin kurumda bir ihtiyaç olduğu düşüncesi ve birilerinin bir şeyler yapması gerektiği bilinci mevcuttur. Süreçler, benzeri işlerin informal olarak ve sezgisel bir şekilde; ancak farklı kişilerce, farklı yerlerde ve farklı prosedürlere dayanılarak yapıldığı, ortak araç ve işleyişin yer almadığı bir seviyede yerine getirilmektedir. Böylelikle kimi süreçler tekrarlanır, kimileri izlenmeye dahi başlanmamış bir durumdadır. Formal bir eğitim veya standardize edilmiş prosedürlere dayanarak bir iletişim ortamı mevcut olmamakla beraber, sorumluluklar kişinin kendisine bırakılmış haldedir.

---

[256] COBIT 4.1, IT Governance Insitute, http://isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm (16 Aralık 2008), s.17

[257] Altuğ Kul, "COBIT'te Olgunluk Seviyelerinin Anlamı ve Hesaplanması", Deloitte Kurumsal Hizmetler Yayını, http://www.denetimnet.net/UserFiles/Documents/DeloitteMakaleleri/Altu%C4%9F_Kul_Makale_Haziran_2007.pdf (12 Haziran 2007).

Kişiye bağımlılık üst seviyede ve kişilerin bilgilerine güvenilerek gerçekleşen bu süreçlerde hata ihtimali yüksektir ancak; genel konularda tutarlı bir iletişim ortamı ve ihtiyacın yerine getirilmesi yönünde ortak bir görüş oluşmuştur.

3-Tanımlanmış Süreç (Defined): Harekete geçilmesi gerektiği anlaşılmış ve kabul edilmiştir. Prosedürler standart hale getirilmiş, dokümante edilmiş ve uygulanmaktadır. Kurallar duyurulmakta, informal eğitimler gerçekleştirilmektedir. Prosedürler karmaşık ve komplike değil, sadece yapılan işe resmiyet kazandırır şekildedir. Araçlar standarttır, ancak eldeki teknikler kullanılmaktadır. Bu seviyede, eğitim almak, standartları takip etmek ve uygulamak her halükarda kişiye bırakılmıştır. Çoğu süreçler bazı metrikler üzerinden izlenmekte ise de, ölçütler sonucu ortaya çıkan sapmalara karşın alınan önlemlerin de kişi bağımlı olması nedeniyle, sapmaların/problemlerin yönetim tarafından tespit edilme ihtimali düşük seviyededir. Kök sebep analizi yapmak ara sıra akla gelmektedir.

4- Yönetilir ve Ölçümlenir (Managed and measurable): Her seviyede sorunlar ve ele alınacak konular tam olarak anlaşılmış ve resmileşmiş eğitimlerle desteklenmektedir. Sorumluluklar net olarak tanımlanmış, süreç sahipliliği kavramı yerleştirilmiştir. Süreçlerin etkin ve/veya verimli işlemediği durumların tespit edilerek iyileştirilmesine yönelik eyleme geçilmesini sağlayacak süreç ve prosedür ölçüm yöntemleri ve metrikler mevcuttur. İyileştirmeler her türlü tespit ve ölçümde olmasa da, çoğu konuda yerine getirilmektedir. Geleneksel olarak kullanılan Finansal ve operasyonel ölçütler, performans ölçütlerine göre daha baskın olarak kullanılsa da, yeni kriterler yavaş yavaş uygulanma eğilimindedir. Süreçler bazen iyileştirilmekte ve kurum içi en iyi uygulamaların örnek alınması zorunluluk haline gelmektedir. Kök sebep analizi standardize edilmiştir. Sürekli iyileştirme kavramı yavaş yavaş gündeme gelmektedir. Kontrollere ilişkin pratikler ve uygulamalar gittikçe daha şeffaflaşır, esnek ve ölçeklenebilir hale gelmektedir. Teknoloji kullanımı sınırlıdır, daha çok taktik anlamda ve belirlenen olgun teknikler ve kullanımı zorunlu standart araçlara dayalıdır. Bilgi teknolojileri stratejisi, kurumun stratejisi ile gün geçtikçe artan bir trend ile uyum sağlamaktadır. Tüm gerekli iç faaliyet alanlarından sorumlu uzmanların katılımı ve paylaşımı göze çarpmaktadır.

5- Optimize Edilmiş (Optimised): Çözümler ve problemler gelişmiş ve ileriye yönelik bir bakış açısı ile anlaşılmaktadır. Eğitim ve iletişim en çağdaş kavram ve tekniklerle yerine getirilmektedir. Performansın izlenmesi için kurumda her türlü iletişim yolları kullanılarak hedefler belirtilmiş ve metrikler tanımlanmıştır. Dışarıdaki kurumlarda örnek olan en iyi uygulamalar kuruma sürekli iyileştirme ve olgunluğu modelleme amaçlı olarak kazandırılmış, süreçler aynı doğrultuda sadeleştirilmiştir. Bu şekilde insan kaynağı, organizasyon ve süreçlerin adaptasyonu hızlanmıştır. Bilgi teknolojileri stratejisi ile kurumun iş stratejisi arasında tam bir uyum sağlanmış ve iş odaklı bir kültürün yerleşmesi doğrultusunda, iş süreçleri iyileştirilir ve yeni iş fırsatları yaratılır hale gelmiştir. Tüm problemler ve hedeflerden sapmalar kök sebep analizi yapılarak incelenmekte, verimli bir şekilde bu problem ve sapma nedenlerini ortadan kaldırma çalışmaları yürütülmektedir. Bilgi teknolojileri, kurumsal boyutta kalite ve etkinliği arttırmak için yaygın, entegre ve optimize edilmiş araçlar olarak kullanılmakta; stratejik bir kaldıraç etkisi yaratarak iş akışlarının otomasyonunu sağlamaktadır. Kurum dışı uzmanlar ve kıyaslama sonuçları rehber niteliğinde kullanılmaktadır. Kontrol uygulamaları zorunlu hale getirilmiş ve sürekli iyileşmeyi sürdürmektedir. Bilgi teknolojileri performans ölçümleri finansal kriterler, müşteri memnuniyeti, operasyonel etkinlik ve ilerde gerekecek yeteneklerin geliştirilmesi boyutlarını dikkate almaktadır.

3.1.1. AHS Yöntemiyle Alt Faktörlerin Göreli Önem Derecelerinin Bulunması

Çalışmada, bankaların operasyonel risk yönetim seviyesini ölçerken 4 ana faktör (insan, süreç, sistem, dış faktörler) grubundan her bir kurumun elde ettiği değerlerden hareketle her bir kurumun toplam operasyonel risk yönetim seviyesi belirlenmiştir. Söz konusu 4 ana faktör, Basel-II kapsamında operasyonel riskin tanımı doğrultusunda oluşturulmuş olup her bir ana faktörün toplam operasyonel risk yönetim olgunluk seviyesi içerisinde eşit ağırlığı varken çalışmada, her bir ana faktör grubu altında yer alan alt faktörlerin birbirlerine göre farklı ağrılıkları vardır. Dolayısıyla, her ana faktör içerisindeki yer alan alt faktörlerin göreli önem derecelerini belirlemek amacıyla çok ölçütlü karar verme yaklaşımlarından olan “Analitik Hiyerarşi Süreci” kullanılmıştır.

Analitik hiyerarşi süreci insanoğlunun hiçbir şekilde kendisine öğretilmeyen fakat varoluşundan bu yana karar verme sorunu ile karşılaştığında içgüdüsel olarak benimsediği

karar mekanizmasıdır[258].Karmaşık yapıdaki ekonomik veya çevresel sorunlara ilişkin çalışmalarda çok sık olarak kullanılmakta olan ölçütlü karar verme yaklaşımlarındandır. AHS ile karşımızdaki problem sistematik bir şekilde gerçekleştirilen ikili değerlendirme ve karşılaştırmalar vasıtasıyla ve nitel ve nicel sahip olunan tüm bilgi ve tecrübeler göz önünde tutularak hiyerarşik bir sınıflandırmaya dönüştürülmektedir. AHS'nin en önemli özelliği, elde edilen faktör ağırlıklarının alt faktörler arasındaki ikili karşılaştırmalar ve değerlendirmeler vasıtasıyla elde edilmesidir. İkili karşılaştırmalarda ilk sorulan soru "Bu iki alt faktörden hangisi önemlidir?" ve takiben ikinci soru da "Ne kadar önemlidir?[259]

AHS'nin diğer önemli özellikleri ise kısaca[260]:

a) Grupların karar alma sürecinde elverişlidir,
b) Kolay kullanımı için gerekli yazılım ve eğitim dokümantasyonu mevcuttur,
c) AHS'nin kullanıldığı çok sayıda akademik çalışma mevcuttur,
d) Deneklerin tercihleri arasındaki uyumu ve tutarlılığı ölçer,
e) Nitel ve nicel çeşitli veriler kullanır,
f) Bireysel ve subjektif kararların verilmesi gereken durumlarda kullanılır.

Diğer taraftan AHS kullanımına ilişkin getirilen bazı eleştiriler şu şekilde özetlenebilir:

a) Faktörlerin arasındaki öncelik ve önemlilik düzeyini belirleyen teorik bir temel olmadığı için aynı kişiler başka bir zamanda daha farklı bir önemlilik sıralaması gerçekleştirebilir,
b) Bireysel olarak belirtilen ağırlıkların kümüle hale dönüştürülmesinde zafiyetler oluşabilir.

Bu adımda oluşturulan uzman ekipten AHS yöntemi kullanarak anketin dört bölümü altında yer alan soruların göreli önem derecelerini bulmaları talep edilmiştir. Kriterlerin içerdikleri anlam konusunda, uygulama sürecinde farklı yorumlar yapılmasını önlemek amacıyla, her kriter tanımlanmış bu tanımlamalar uygulama esnasında değerlendirmeyi yapan uzman ekibe açıklanmıştır.

---

[258] T.L. Saaty, **Fundamentals of Decision Making and Priority Theory with Analytic Hierarchy Process**, AHP Series, Vol: VI, RWS Publications, 2000.
[259] Carreño ve Diğerleri, s.6, http://www.unisdr.org/HFdialogue/download/tp1-Evaluation-risk-management-performance-m1.pdf (12 Ocak 2009).
[260] J.E. De Steiguer, Jennifer Duberstein ve Vicente Lopes, "The Analytic Hierarchy Process as a Means for Integrated Watershed Management", http://www.tucson.ars.ag.gov/ICRW/Proceedings/Steiguer.pdf (20 Mart 2009).

İçgüdüsel mekanizma, karar sürecinde doğal olarak niteliksel kriterleri de göz önünde bulundurmaktadır. Bu sebeple AHS'nin gücü, diğer çoğu yaklaşımla ele alınması zor veya mümkün olmayan ama kararları etkileyen bu gibi etkenleri de ele alabilmesinden kaynaklanmaktadır. Aşağıda AHS felsefesinin kullanımında izlenen yol ana hatlarıyla açıklanmaktadır.

1. Farklı kriterlerin Tablo 18'de gösterildiği gibi ikili karşılaştırmaları yapılarak bir matris oluşturulur. Matristeki X_i / X_j terimi, amaca ulaşmak için *i.* kriterin *j.* kriterden ne kadar daha önemli olduğunu ifade etmektedir.

Tablo 18: Kriterler için İkili Karşılaştırmalar Matrisi Oluşturulması

	Kriter 1	**Kriter 2**	**Kriter n**
Kriter 1	X_1/X_1	X_1/X_2	X_1/X_n
Kriter 2 .	X_2/X_1	X_2/X_2.....	X_2/X_n
Kriter n	X_n/X_1	X_n/X_2	X_n/X_n

Kaynak: T.L Saaty, **"Analytical Planning"**, RWS Publications, 1985

Bu değerlendirmede Tablo 19'da gösterilen ölçek kullanılmaktadır. Örneğin bu değer 5 ise, *i.* kriterin *j.* kritere göre *"kuvvetli düzeyde"* önemli olduğu anlaşılmaktadır. Bu durumda benzer şekil *j.* kriter de *i.* kritere göre 1/5 düzeyinde önemli olmaktadır.

Tablo 19: Analitik Hiyerarşi Sürecinde Kullanılan Ölçek

ÖNEM DERECESİ	TANIM	AÇIKLAMA
1	Eşit düzeyde önem	İki kriter amaca eşit düzeyde katkıda bulunuyor
3	Birinin diğerine göre orta derecede daha önemli olması	Tecrübe ve yargı bir faaliyeti diğerine göre orta derecede tercih ettiriyor.
5	Kuvvetli düzeyde önem	Tecrübe ve yargı bir faaliyeti diğerine göre kuvvetli bir şeklide tercih ettiriyor.
7	Çok kuvvetli düzeyde önem	Bir faaliyet güçlü bir şekilde tercih ediliyor ve baskınlığı uygulamada rahatlıkla görülüyor.
9	Aşırı düzeyde önem	Bir faaliyetin diğerine tercih edilmesine ilişkin kanıtlar büyük bir güvenilirliğe sahip
2,4,6,8	Ortalama değerler	Uzlaşma gerektirdiğinde kullanılmak üzere iki ardışık yargı arasına düşen değerler

Kaynak: T.L Saaty, **"Analytical Planning"**, RWS Publications, 1985

2. Kriterlerin göreli önemleri bulunarak matris tutarlılığı hesaplanır. Bir karşılaştırma matrisinin tutarlı olabilmesi için, en büyük özdeğerinin (λ_{max}) matris boyutuna *(n)* eşit olması gerekmektedir. Kriterlerin göreli önemlerini hesaplamak için, her bir satırın geometrik ortalaması alınarak *"X_i"* sütun vektörü oluşturulur. Oluşturulan sütun vektörü normalize edilerek, göreli önemler vektörü *"NX_i"* hesaplanır. Matristeki her bir satır göreli önemler vektörü ile çarpılarak V_2 sütun vektörü elde edilir. Daha sonra bu vektörün her elemanı, göreli önemler vektöründe karşı gelen elemana bölünerek V_3 vektörü hesaplanmakta, V_3 sütun vektörünün aritmetik ortalaması ise en büyük özdeğer olan λ_{max}'ı vermektedir.

3. Son adım, tutarlılık göstergesinin ve tutarlılık oranının bulunmasıdır. Bu değerler;

$$TutarlılıkGöstergesi = \frac{\lambda_{\max} - n}{n-1} \qquad \textbf{(11)}$$

$$TutarlılıkOranı = \frac{TutarlılıkGöstergesi}{RassallıkGöstergesi} \qquad \textbf{(12)}$$

ifadeleriyle hesaplanmaktadır. Tutarlılık oranının 0.1'den küçük çıkması halinde matrisin tutarlı olduğu kabul edilir.

Yapılan bir çalışma sonucu 1-15 boyutundaki matrisler için rassallık göstergeleri Tablo 20'de gösterilmektedir[261]. Tabloda yer alan "*n*" matris boyutudur.

Tablo 20:Rassallık Göstergeleri

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Rassallık Göstergesi	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,59

Kaynak: T.L Saaty, "Analytical Planning", RWS Publications, 1985

3.1.1.1. "İNSAN" Altındaki Faktörlerin Ağırlıklandırılması

Anketin dört ana bölümünün her biri altında yer alan alt faktörler kendi içerisinde AHS ile ağırlıklandırılmıştır. Her bir alt faktöre ait değerlendirme cümleleri birbirleriyle ikili karşılaştırmalar yapılmış ve elde edilen matrisin tutarlılığı test edilmiştir. Değerlendirme ifadelerinin birbirlerine göre göreli önem dereceleri uzman ekibin verdiği cevaplar doğrultusunda AHS yöntemiyle belirlenmiştir. Bölüm içerisindeki kriterler sırayla ikili karşılaştırmalara tabi tutulmuş, uzman ekibin her bir ikili karşılaştırmaya verdikleri cevapların aritmetik ortalaması AHS matrisine yerleştirilip bütün kriterler için matrisin tutarlılık testi yapılmıştır. Tutarsızlık durumunda uzman ekibin kriterlere verdikleri önem derecelerini gözden geçirmeleri istenmiştir. Bu uygulama matris tutarlılık testinden geçene kadar devam etmiştir. Oluşan matris Tablo 21'de yer almaktadır.

[261] T.L Saaty, **Analytical Planning**, RWS Publications, 1985.

Tablo 21: "İNSAN" Kaynaklı Operasyonel Risk Yönetim Uygulamaları Bölümüne Ait Soruların İkili Karşılaştırma Değerleri ve Tutarlılık Testi

İNSAN	IK01	IK02	IK03	IK04	IK05	IK06	X_i	NX_i	V_2	V_2 / NX_i
IK01	**1**	**4**	1/2	**1**	**2**	**3**	1.51	0.21	1.25	6.04
IK02	1/4	**1**	1/5	1/4	1/3	1/2	0.36	0.05	0.30	6.11
IK03	**2**	**5**	1	**2**	**3**	**4**	2.49	0.33	2.08	6.10
IK04	**1**	**4**	1/2	1	**2**	**3**	1.51	0.21	1.25	6.04
IK05	1/2	**3**	1/3	1/2	1	**2**	0.89	0.12	0.74	6.07
IK06	1/3	**2**	1/4	1/3	1/2	1	0.55	0.08	0.46	6.07
							7.32	1.00	1.00	λ_{max}=6.07

n=6(ifadeler) $TutarlılıkGöstergesi = \frac{\lambda_{\max} - n}{n-1}$ =(6.07-6)/(6-1) =0.01

$TutarlılıkOranı = \frac{TutarlılıkGöstergesi}{RassallıkGöstergesi}$ =0.01 / 1.24 = **0.01<0.1**➔matris tutarlıdır.

Sonuçta anketin "İNSAN" faktörü ana bölümü içerisinde yer alan Tablo 22'de sıralanan alt faktörlerin bölüm içerisindeki göreli önem dereceleri (ağırlıkları) belirlenmiştir.

Tablo 22: "İNSAN" Faktörüne Ait Değerlendirme İfadeleri

ALT FAKTÖR	KATSAYI (%)	DEĞERLENDİRME İFADESİ
IK01	21	İnsan Kaynakları Yönetim Metodolojisi
IK02	5	Eğitim Politikası
IK03	33	Suiistimallerin Önlenmesi ve Etik İlkelere Uyum
IK04	21	Görev Tanımları
IK05	12	Personel İşe Alım- İşten Ayrılış Süreci
IK06	8	Performans Yönetimi
TOPLAM	100	

3.1.1.2. "SİSTEM" Altındaki Faktörlerin Ağırlıklandırılması

"Sistem" faktörü altında yer alan 8 adet alt faktör değerlendirme cümleleri uzman ekip tarafından birbirleriyle ikili karşılaştırmalara tabi tutulmuş, birbirlerine göre göreli önem dereceleri uzman ekibin verdiği cevaplar doğrultusunda AHS yöntemiyle belirlenmiştir.

Uzman ekibin aynı iki kriter karşılaştırması için verdikleri göreli önem derecelerinin aritmetik ortalaması alınarak ekibin söz konusu iki kriter için verdiği ortalama önem derecesi notuna ulaşılmıştır. Bu notların ortalamaları tam sayıya yuvarlanarak AHS matrisine yerleştirilmiştir.

AHS matrisine yerleştirilen bütün kriterler için matrisin tutarlılık testi yapılmıştır. Tutarsızlık durumunda uzman ekibin kriterlere verdikleri önem derecelerini gözden geçirmeleri istenmiştir. Bu uygulama matris tutarlılık testinden geçene kadar devam etmiştir. Oluşan AHS matrisi Tablo 23'de yer almaktadır.

Tablo 23: "SİSTEM" Kaynaklı Operasyonel Risk Yönetim Uygulamaları Bölümüne Ait Soruların İkili Karşılaştırma Değerleri ve Tutarlılık Testi

SİSTEM	SI01	SI02	SI03	SI04	SI05	SI06	SI07	SI08	X_i	NX_i	V_2	V_2 / NX_i
SI01	**1**	1/2	1/3	1/2	1/3	1/5	1/4	1/4	0.37	0.04	0.31	8.23
SI02	**2**	**1**	1/2	1	1/2	1/4	1/3	1/3	0.59	0.06	0.48	8.09
SI03	**3**	**2**	**1**	**2**	1/3	1/3	1/2	1/2	1.00	0.10	0.82	8.04
SI04	**2**	**1**	1/2	**1**	1/2	1/4	1/4	1/4	0.55	0.06	0.45	8.12
SI05	**3**	**2**	1	2	**1**	1/3	1/3	1/3	0.90	0.09	0.75	8.21
SI06	**5**	**4**	3	4	3	**1**	2	2	2.71	0.27	2.26	8.21
SI07	**4**	**3**	2	4	3	1/2	**1**	1	1.86	0.19	1.55	8.17
SI08	**4**	**3**	2	4	3	1/2	1	**1**	1.86	0.19	1.55	8.17
									9.83	1.00		λ_{max}=8.16

n=8(ifadeler) $TutarlılıkGöstergesi = \frac{\lambda_{\max} - n}{n-1}$ **=**(8.16-8)/(8-1) =0.02

$TutarlılıkOranı = \frac{TutarlılıkGöstergesi}{RassallıkGöstergesi}$ = 0.02 / 1.41 = **0.02<0.1**➔matris tutarlıdır.

Sonuçta anketin “SİSTEM” faktörü ana bölümü içerisinde yer alan Tablo 24’de sıralanan alt faktörlerin bölüm içerisindeki göreli önem dereceleri (ağırlıkları) belirlenmiştir.

Tablo 24: “SİSTEM” Faktörüne Ait Değerlendirme İfadeleri

ALT FAKTÖR	KATSAYI (%)	DEĞERLENDİRME İFADESİ
SI01	4	Bilgi Teknolojileri Risk Tanımlama ve Değerlendirme
SI02	6	Bilgi Teknolojileri Alt Yapısının Yenileme ve Bakımı
SI03	10	Uygulamaların Test Edilmesi
SI04	6	Bilgi Teknolojileri Performans ve Kapasite Yönetimi
SI05	9	Değişiklik Yönetimi
SI06	27	Bilgi Teknolojileri İş Süreklilik Planı
SI07	19	Bilgi Güvenlik Politikası
SI08	19	Bilgi Güvenlik Test ve Analizleri
TOPLAM	100	

3.1.1.3. “SÜREÇ” Altındaki Faktörlerin Ağırlıklandırılması

“Süreç” faktörü altında yer alan 12 adet alt faktör değerlendirme cümleleri uzman ekip tarafından birbirleriyle ikili karşılaştırmalara tabi tutulmuş, birbirlerine göre göreli önem dereceleri uzman ekibin verdiği cevaplar doğrultusunda AHS yöntemiyle belirlenmiştir.Uzman ekibin aynı iki kriter karşılaştırması için verdikleri göreli önem derecelerinin aritmetik ortalaması alınarak ekibin söz konusu iki kriter için verdiği ortalama önem derecesi notuna ulaşılmıştır. Bu notların ortalamaları tam sayıya yuvarlanarak AHS matrisine yerleştirilmiştir.

AHS matrisine yerleştirilen bütün kriterler için matrisin tutarlılık testi yapılmıştır. Tutarsızlık durumunda uzman ekibin kriterlere verdikleri önem derecelerini gözden geçirmeleri istenmiştir. Bu uygulama matris tutarlılık testinden geçene kadar devam etmiştir.Oluşan AHS matrisi Tablo 25’de yer almaktadır.

Tablo 25: "SÜREÇ" Kaynaklı Operasyonel Risk Yönetim Uygulamaları Bölümüne Ait Soruların İkili Karşılaştırma Değerleri ve Tutarlılık Testi

SÜREÇ	SU01	SU02	SU03	SU04	SU05	SU06	SU07	SU08	SU09	SU10	SU11	SU12	X_i	NX_i	V_2	V_2 / NX_i
SU01	**1**	**2**	1/3	1/3	**1**	1/4	1/2	**3**	**4**	1/2	1/2	**3**	0.89	0.06	0.72	12.67
SU02	1/2	**1**	1/4	1/4	1/6	1/5	1/3	**2**	**3**	1/2	1/3	**2**	0.55	0.03	0.44	12.58
SU03	**3**	**4**	**1**	**1**	**1**	**2**	**2**	**5**	**6**	**2**	**2**	**5**	2.35	0.15	1.94	12.94
SU04	**3**	**4**	**1**	**1**	**1**	1/2	**2**	**5**	**6**	**2**	**2**	**5**	2.10	0.13	1.65	12.37
SU05	**1**	**6**	**1**	**1**	**1**	**1**	**1**	**5**	**6**	**1**	**1**	**5**	1.76	0.11	1.45	12.88
SU06	**4**	**5**	**2**	**2**	**1**	**1**	**3**	**6**	7	**3**	**3**	**6**	3.01	0.19	2.44	12.76
SU07	**2**	**3**	1/2	1/2	**1**	1/3	**1**	**4**	**5**	**1**	**1**	**4**	1.36	0.09	1.07	12.30
SU08	1/3	1/2	1/5	1/5	1/5	1/6	1/4	**1**	1/2	1/5	1/4	**1**	0.33	0.02	0.26	12.62
SU09	1/4	1/3	1/6	1/6	1/6	1/7	1/5	**2**	**1**	1/5	1/4	1/2	0.30	0.02	0.25	12.89
SU010	**2**	**2**	1/2	1/2	**1**	1/3	**1**	**5**	**5**	**1**	**1**	**4**	1.34	0.09	1.05	12.33
SU011	**2**	**3**	1/2	1/2	**1**	1/3	**1**	**4**	**4**	**1**	**1**	**4**	1.33	0.09	1.05	12.31
SU012	1/3	1/2	1/5	1/5	1/5	1/6	1/5	**1**	**2**	1/4	1/4	**1**	0.37	0.02	0.29	12.43
													15.7	1.00		λ_{max}=12.59

n=12(ifadeler) $TutarlılıkGöstergesi = \frac{\lambda_{\max} - n}{n-1}$ **=**(12.59-12)/(12-1) =0.05

$TutarlılıkOranı = \frac{TutarlılıkGöstergesi}{RassallıkGöstergesi}$ = 0.05 / 1.48 = **0.04<0.1**➔matris tutarlıdır.

Sonuçta anketin "SÜREÇ" faktörü ana bölümü içerisinde yer alan Tablo 26'da sıralanan alt faktörlerin bölüm içerisindeki göreli önem dereceleri (ağırlıkları) belirlenmiştir.

Tablo 26: "SÜREÇ" Faktörüne Ait Değerlendirme İfadeleri

ALT FAKTÖR	KATSAYI (%)	DEĞERLENDİRME İFADESİ
SU01	6	Operasyonel Risk Yönetiminde Kurum Kültürü
SU02	3	Operasyonel Risk Kayıp Veritabanı
SU03	15	Operasyonel Riskin Tanımlanması ve Değerlendirilmesi
SU04	13	Operasyonel Riskin Ölçülmesi
SU05	11	Operasyonel Riske Karşı Aksiyon Alınması
SU06	19	İç Kontrol Sistemi
SU07	9	Kurumsal Risk Yönetimi
SU08	2	Proje Geliştirme
SU09	2	Kalite Yönetimi
SU010	9	Kontrollere İlişkin Dokümantasyon
SU011	9	Operasyonel İşlem Limitlerinin Belirlenmesi
SU012	2	Problem Yönetimi
TOPLAM	100	

3.1.1.4. "DIŞSAL ETKENLER" Altındaki Faktörlerin Ağırlıklandırılması

"DIŞSAL ETKENLER" faktörü altında yer alan 7 adet alt faktör değerlendirme cümleleri uzman ekip tarafından birbirleriyle ikili karşılaştırmalara tabi tutulmuş, birbirlerine göre göreli önem dereceleri uzman ekibin verdiği cevaplar doğrultusunda AHS yöntemiyle belirlenmiştir. Uzman ekibin aynı iki kriter karşılaştırması için verdikleri göreli önem derecelerinin aritmetik ortalaması alınarak ekibin söz konusu iki kriter için verdiği ortalama önem derecesi notuna ulaşılmıştır. Bu notların ortalamaları tam sayıya yuvarlanarak AHS matrisine yerleştirilmiştir.

AHS matrisine yerleştirilen bütün kriterler için matrisin tutarlılık testi yapılmıştır. Tutarsızlık durumunda uzman ekibin kriterlere verdikleri önem derecelerini gözden geçirmeleri istenmiştir. Bu uygulama matris tutarlılık testinden geçene kadar devam etmiştir. Oluşan AHS matrisi Tablo 27'de yer almaktadır.

Tablo 27: "DIŞSAL ETKENLER" Kaynaklı Operasyonel Risk Yönetim Uygulamaları Bölümüne Ait Soruların İkili Karşılaştırma Değerleri ve Tutarlılık Testi

DIŞSAL ETKEN	DI01	DI02	DI03	DI04	DI05	DI06	DI07	X_i	NX_i	V_2	V_2 / NX_i
DI01	**1**	1/5	1/3	1/4	1/4	1/2	1/6	0.32	0.04	0.27	7.12
DI02	**5**	**1**	**3**	**2**	**2**	**4**	**1**	2.19	0.25	1.80	7.07
DI03	**3**	1/3	**1**	1/2	1/2	**2**	1/3	0.77	0.09	0.64	7.11
DI04	**4**	1/2	**2**	**1**	**1**	**3**	1/3	1.22	0.14	1.02	7.16
DI05	**4**	1/2	**2**	1	**1**	**3**	1/2	1.29	0.15	1.06	7.06
DI06	**2**	1/4	1/2	1/3	1/3	**1**	1/3	0.51	0.06	0.43	7.19
DI07	**6**	**1**	**3**	**3**	**2**	**3**	**1**	2.28	0.27	1.92	7.22
								8.59	**1.00**		**λ_{max}=7.13**

n=7(ifadeler) $TutarlılıkGöstergesi = \frac{\lambda_{\max} - n}{n-1}$ **=**(7.13-7)/(7-1) =0.02

$TutarlılıkOranı = \frac{TutarlılıkGöstergesi}{RassallıkGöstergesi}$ = 0.02/1.32 = **0.02<0.1➔**matris tutarlıdır.

Sonuçta anketin "DIŞSAL ETKENLER" faktörü ana bölümü içerisinde yer alan Tablo 28'de sıralanan alt faktörlerin bölüm içerisindeki göreli önem dereceleri (ağırlıkları) belirlenmiştir.

Tablo 28: "DIŞSAL ETKENLER" Faktörüne Ait Değerlendirme İfadeleri

ALT FAKTÖR	KATSAYI (%)	DEĞERLENDİRME İFADESİ
DI01	4	Tedarikçi Performans Değerlendirmesi
DI02	25	İş Sürekliliğinin Sağlanması
DI03	9	Acil Durum ve İş Süreklilik Planı Testleri
DI04	14	Elektronik Veri ve Kritik Dokümanların Yedeklenmesi
DI05	15	Acil Durum Merkezinin Kurulması
DI06	6	Acil Durum ve İş Süreklilik Eğitimleri
DI07	27	Fiziksel ve Çevresel Güvenlik
TOPLAM	100	

3.2. ORYOS Endeksinin Oluşturulması

Çalışmanın temel amacı gerek tüm bankacılık sektörü, gerek sahiplik veya faaliyet açısından gruplanan banka türleri gerekse de münferit olarak her banka için operasyonel risk yönetim olgunluk seviyelerini ölçebilecekleri ortak bir ölçek/gösterge tasarlayarak söz konusu gösterge ile bir zaman serisi içerisinde belli periyotlarda ölçümler gerçekleştirerek bunu bir endeks gibi kullanmak böylece operasyonel risk yönetiminin zaman içerisindeki performansını ve dolayısıyla etkinliğini kendileri, banka grupları ve sektör açısından ölçebilme ve karşılaştırma yapabilme imkanı sağlamaktır.

Sonuçta münferit olarak her banka veya banka grubu ya da sektör için elde edilen operasyonel risk yönetimi olgunluk seviyesi endeksini (ORYOS) denetleyici ve düzenleyici otoriteler baz alarak bunu bankaların Basel-II'de operasyonel riskler için ayırmaları gereken sermaye yükümlülük hesabında kullanabilirler.

ORYOS ile münferit olarak bankaların veya sahiplik (kamu, yabancı, yerli özel)/faaliyet(mevduat, kalkınma&yatırım, katılım) açısından gruplanan bankaların ya da tüm bankacılık sektörünün belirli periyotlarda yapılacak operasyonel risk yönetimi olgunluk seviyesi ölçümleri ile ortaya çıkan endeks değerleri karşılaştırılarak bankaların hedeflenen seviyelere yaklaşma performansları yada birbirlerine, banka gruplarına veya sektör ortalamasına göre mukayese yapma olanağı olacaktır.

Bankaların operasyonel risk yönetimi olgunluk seviyesinin belirlenmesine yönelik olarak hazırlanmış anket dört ana bölümden oluşmaktadır. Anketin bölümleri Basel-II kapsamında operasyonel riskin tanımı içerisinde yer alan ve bu riskin temel kaynakları sayılan alanlardır. İnsan faktörüyle ilişkilendirilen operasyonel risk yönetimi olgunluk seviyesi $ORYOS_{insan}$, sistem faktörüyle ilişkilendirilen operasyonel risk yönetimi olgunluk seviyesi $ORYOS_{sistem}$, süreç faktörüyle ilişkilendirilen operasyonel risk yönetimi olgunluk seviyesi $ORYOS_{süreç}$, ve dış faktör ile ilişkilendirilen operasyonel risk yönetimi olgunluk seviyesi $ORYOS_{dışsal}$ olarak belirlenmiştir. ORYOS, sayılan bu dört ana parçanın aritmetik ortalamasından oluşmaktadır.

$$\mathbf{ORYOS = (ORYOS_{insan} + ORYOS_{sistem} + ORYOS_{süreç} + ORYOS_{dışsal})/4} \qquad \mathbf{(13)}$$

$ORYOS_{insan}$ faktör grubu için kurumun olgunluk seviyesinin belirleneceği 6 adet gösterge (alt faktör) belirlenmiştir. $ORYOS_{sistem}$ faktör grubu altında 8 adet, $ORYOS_{süreç}$ faktör grubu 12 adet, $ORYOS_{dışsal}$ faktör grubu altında 7 adet gösterge belirlenmiştir. Her bir faktör grubu için çok daha fazla sayıda gösterge belirlenmesi mümkün olmasına karşın anketin mevcut haliyle operasyonel risk yönetim seviyesini anlamlı bir sonuç elde etmeye yetecek içerikte olduğu düşünüldüğü ve diğer taraftan da anketin anlamlı ve makul biçimde cevaplanabilmesi ve geri dönüşünün sağlanabilmesi amacıyla faktörlere ilişkin gösterge sayıları arttırılmamıştır.

Her faktör grubu altında yer alan göstergelerin her birisi için COBIT metodolojisi kapsamındaki jenerik olgunluk modelinden esinlenerek oluşturulan göstergeler, sıfır(0:yok) ile beş (5:optimum) arasında değişen 6 farklı seviyedeki olgunluk seviyelerini ifade etmektedir. Bu şekilde hazırlanmış olan metodoloji ile her bir olgunluk seviyenin eşzamanlı olarak bir "performans hedefi" olarak kullanılması, karşılaştırma ve değerlendirme yapabilme olanağı mevcuttur. Bankalar, her bir faktör grubu altında yer alan göstergelerden hareketle mevcut durumlarını değerlendirebilecek ve hangi seviyeye ulaşmak istediklerini belirleyerek politika ve stratejilerini buna göre belirleyebileceklerdir.

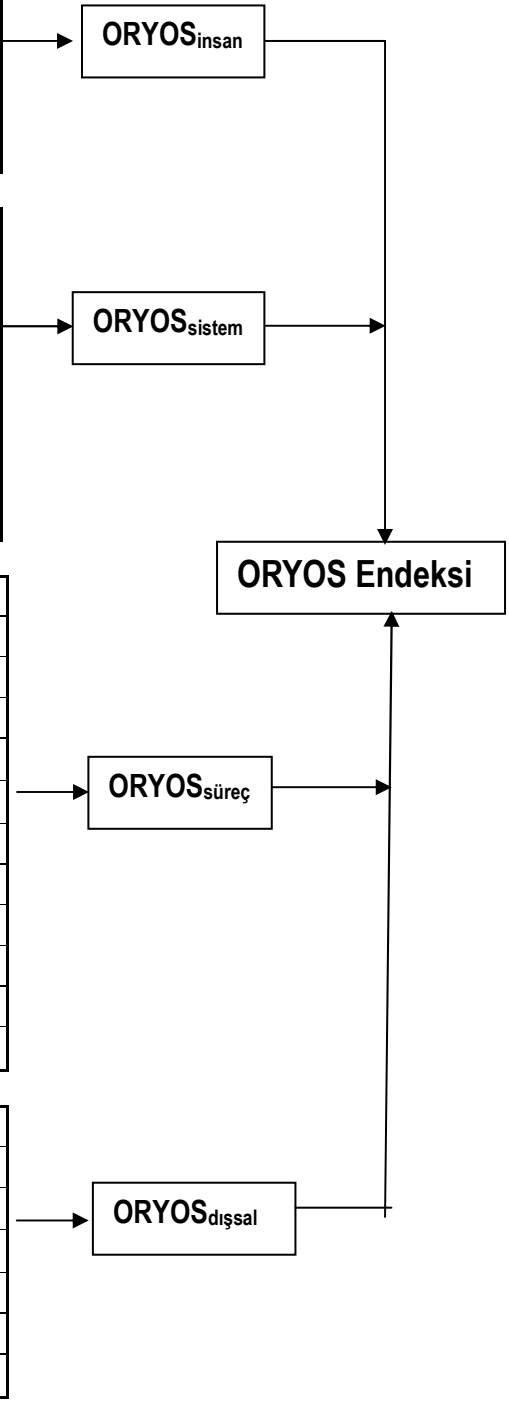
Aşağıda yer alan Şekil 9'da operasyonel risk yönetim olgunluk seviyesi endeksi hesaplamasında kullanılacak dört ana faktör ve bunların altında yer alan 33 adet alt faktör isimleri ile birlikte belirtilmiştir.

İNSAN	IK01	İnsan Kaynakları Yönetim Metodolojisi	W_{IK01}
	IK02	Eğitim Politikası	W_{IK02}
	IK03	Suiistimallerin Önlenmesi ve Etik İlkelere Uyum	W_{IK03}
	IK04	Görev Tanımları	W_{IK04}
	IK05	Personel İşe Alım- İşten Ayrılış Süreci	W_{IK05}
	IK06	Performans Yönetimi	W_{IK06}

SİSTEM	SI01	BT Risk Tanımlama ve Değerlendirme	W_{SI01}
	SI02	Bilgi Teknolojileri AltYapı Yenileme&Bakım	W_{SI02}
	SI03	Uygulamaların Test Edilmesi	W_{SI03}
	SI04	Bilgi Teknoloji Performans&Kapasite Yönetimi	W_{SI04}
	SI05	Değişiklik Yönetimi	W_{SI05}
	SI06	Bilgi Teknolojileri İş Süreklilik Planı	W_{SI06}
	SI07	Bilgi Güvenlik Politikası	W_{SI07}
	SI08	Bilgi Güvenlik Test ve Analizleri	W_{SI08}

SÜREÇ	SU01	Operasyonel Risk Yönetiminde Kurum Kültürü	W_{SU01}
	SU02	Operasyonel Risk Kayıp Veritabanı	W_{SU02}
	SU03	Operasyonel Risk Tanımlama&Değerlendirme	W_{SU03}
	SU04	Operasyonel Riskin Ölçülmesi	W_{SU04}
	SU05	Operasyonel Riske Karşı Aksiyon Alınması	W_{SU05}
	SU06	İç Kontrol Sistemi	W_{SU06}
	SU07	Kurumsal Risk Yönetimi	W_{SU07}
	SU08	Proje Geliştirme	W_{SU08}
	SU09	Kalite Yönetimi	W_{SU09}
	SU10	Kontrollere İlişkin Dokümantasyon	W_{SU10}
	SU11	Operasyonel İşlem Limitlerinin Belirlenmesi	W_{SU11}
	SU12	Problem Yönetimi	W_{SU12}

DIŞSAL ETKEN	DF01	Tedarikçi Performans Değerlendirmesi	W_{DF01}
	DF02	İş Sürekliliğinin Sağlanması	W_{DF02}
	DF03	Acil durum ve İş Süreklilik Planı Testleri	W_{DF03}
	DF04	Elektronik Veri ve Kritik Dok.Yedeklenmesi	W_{DF04}
	DF05	Acil Durum Merkezinin Kurulması	W_{DF05}
	DF06	Acil Durum ve İş Süreklilik Eğitimleri	W_{DF06}
	DF07	Fiziksel ve Çevresel Güvenlik	W_{DF07}



Şekil 9: ORYOS'un Dört Ana Faktör ve Otuzüç Alt Faktörü

Şekil 9'da ORYOS'u oluşturan dört ana faktör ve bunlar altında yer alan alt faktörler ile AHS yöntemine göre bulunan alt faktörlerin ağırlık sembolleri gösterilmiştir. Her bir ana faktör altındaki alt faktörlerin ağırlıkları toplamı 1'dir. Aşağıdaki ifadede N her bir faktör grubu altında yer alan gösterge sayısını (alt faktör) ifade etmektedir.

$$\sum_{j=1}^{N} w_j = 1 \qquad \textbf{(14)}$$

Buna göre tek tek ana faktörlerin ORYOS'ları şu şekilde hesaplanmaktadır;

$$\textbf{ORYOS}_{\textbf{insan}}=(\textbf{ORYOS}_{\textbf{IK01*}}\ \textbf{w}_{\textbf{IK01}})+(\textbf{ORYOS}_{\textbf{IK02*}}\ \textbf{w}_{\textbf{IK02}})+\ldots\ldots(\textbf{ORYOS}_{\textbf{IK06*}}\ \textbf{w}_{\textbf{IK06}}) \qquad \textbf{(15)}$$

$$\textbf{ORYOS}_{\textbf{sistem}}=(\textbf{ORYOS}_{\textbf{SI01*}}\ \textbf{w}_{\textbf{SI01}})+(\textbf{ORYOS}_{\textbf{SI02*}}\ \textbf{w}_{\textbf{SI02}})+\ldots\ldots(\textbf{ORYOS}_{\textbf{SI08*}}\ \textbf{w}_{\textbf{SI08}}) \qquad \textbf{(16)}$$

$$\textbf{ORYOS}_{\textbf{süreç}}=(\textbf{ORYOS}_{\textbf{SU01*}}\ \textbf{w}_{\textbf{SU01}})+(\textbf{ORYOS}_{\textbf{SU02*}}\ \textbf{w}_{\textbf{SU02}})+\ldots.(\textbf{ORYOS}_{\textbf{SU12*}}\ \textbf{w}_{\textbf{SU12}}) \qquad \textbf{(17)}$$

$$\textbf{ORYOS}_{\textbf{dışsal}}=(\textbf{ORYOS}_{\textbf{DF01*}}\ \textbf{w}_{\textbf{DF01}})+(\textbf{ORYOS}_{\textbf{DF02*}}\ \textbf{w}_{\textbf{DF02}})+\ldots.(\textbf{ORYOS}_{\textbf{DF07*}}\ \textbf{w}_{\textbf{DF07}}) \qquad \textbf{(18)}$$

Dört ana faktörün toplamı ile de aşağıdaki formülde de gösterildiği üzere bankanın, banka grubunun veya sektörün operasyonel risk yönetim olgunluk seviyesine (ORYOS) ulaşılabilir.

$$\textbf{ORYOS}=\left(\sum_{J=1}^{N} ORYOS_{IKJ}\times W_{IKJ}+\sum_{J=1}^{N} ORYOS_{SIJ}\times W_{SIJ}+\sum_{J=1}^{N} ORYOS_{SUJ}\times W_{SUJ}+\sum_{J=1}^{N} ORYOS_{DFJ}\times W_{DFJ}\right)/4 \qquad \textbf{(19)}$$

Formülde geçen *Wj* her bir faktör grubu içersinde yer alan göstergelerin faktör toplamı içerisindeki ağırlığını göstermekte; $ORYOS_J$ ise bankanın her bir gösterge için mevcut olgunluk seviyesini göstermektedir. Tablo 29'da AHS yöntemiyle bulunan faktörlere ait alt faktör ağırlıkları (%) olarak yer almaktadır.

Tablo 29: ORYOS'un Dört Ana Faktörünün Alt Faktör Ağırlıkları (%)

FAKTÖRLER	W_{01}	W_{02}	W_{03}	W_{04}	W_{05}	W_{06}	W_{07}	W_{08}	W_{09}	W_{10}	W_{11}	W_{12}
$ORYOS_{insan}$	21	5	33	21	12	8						
$ORYOS_{sistem}$	4	6	10	6	9	27	19	19				
$ORYOS_{süreç}$	6	3	15	13	11	19	9	2	2	9	9	2
$ORYOS_{dışsal}$	4	25	9	14	15	6	27					

Çalışmanın sonucunda türleri Tablo 30'da yer alan operasyonel risk yönetim seviyeleri belirlenmiş olacaktır.

Tablo 30: Çalışma Neticesinde Hesaplanacak ORYOS Endeksleri

ENDEKSLER	$ORYOS_{genel}$	$ORYOS_{insan}$	$ORYOS_{sistem}$	$ORYOS_{süreç}$	$ORYOS_{dışsal}$
$ORYOS_{kamu}$	?	?	?	?	?
$ORYOS_{yerli\text{-}özel}$	?	?	?	?	?
$ORYOS_{yabancı}$	?	?	?	?	?
$ORYOS_{mevduat}$	?	?	?	?	?
$ORYOS_{kalk\&yat}$	?	?	?	?	?
$ORYOS_{katılım}$	?	?	?	?	?
$ORYOS_{kamu\text{-}mevduat}$	?	?	?	?	?
$ORYOS_{kamu\text{-}kalk\&yat}$	?	?	?	?	?
$ORYOS_{yerliözel\text{-}mevduat}$	?	?	?	?	?
$ORYOS_{yerliözel\text{-}kalk\&yat}$	?	?	?	?	?
$ORYOS_{yerliözel\text{-}katılım}$	?	?	?	?	?
$ORYOS_{yabancı\text{-}mevduat}$	?	?	?	?	?
$ORYOS_{yabancı\text{-}kalk\&yat}$	?	?	?	?	?
$ORYOS_{sektör}$	?	?	?	?	?

DÖRDÜNCÜ BÖLÜM

4. AMPİRİK ÇALIŞMANIN BULGULARI

Finansal risklerin sayısallaştırılmasında ve bankanın belirlenen zaman dilimi içinde belli bir güven düzeyinde kaybedebileceği değerin hesaplanmasında, riskin gerçekleşme olasılığı ve risk gerçekleştiğinde kaybedilecek tutar üzerinden hesaplamalar yapılmaktadır. Operasyonel riskin sayısallaştırılması amacıyla kullanılan yöntemler de bu temele dayanmakla birlikte bu noktada olasılık hesaplaması ve kaybedilebilecek tutarın belirlenmesi finansal risklere göre daha zor bir süreçtir. Çünkü operasyonel risklerin bir kısmı banka dışındaki değişkenlerden kaynaklanabilmektedir ya da meydana gelen riskler düzenli olarak ortaya çıkan riskler olmamakta, bu durumda ölçümlemelerde güçlük yaşanmasına sebep olmaktadır.

Bu noktadan hareketle sayısallaştırılması diğer riskler gibi kolay olmayan operasyonel risklerle ilgili olarak sektörün ve sektördeki bankaların operasyonel risk yönetimi konusunda ne seviyede olduklarını belirlemeye yönelik olarak olgunluk modeline (CMM: Capability Mature Model) göre hazırlanmış değerlendirme cümleleri bir anket ile bankalara sunulmuştur.

Anket operasyonel riskin kaynağını oluşturan “İNSAN”, “SİSTEM”, “SÜREÇ” ve “DIŞSAL ETKENLER” olmak üzere dört ana bölümden oluşmuştur. Her bir bölüm kendi içinde çeşitli sayıdaki alt faktörlerden oluşan değerlendirme cümlelerinden kurulmuştur. Bu cümlelerin birbirlerine göre göreli önem dereceleri de analitik hiyerarşi süreci (AHP: Analytic Hierarchy Process) yöntemiyle belirlenmiştir.

Böylece her bankadan ankette yer alan toplam 33 adet değerlendirme cümlesi için bu cümleler altında yer alan alt cümlelerden kendi durumlarına en uygun olanı seçmeleri talep edilmiştir. Seçilen seçenekler AHS’ye göre belirlenen göreli önem dereceleri ile ağırlıklandırılarak her bankanın ağırlıklandırılmış olgunluk seviyesine ulaşılmıştır.

Sonuçta hem bankacılık sektörünün, hem de sahiplik ve faaliyet açısından banka gruplarının ***“Operasyonel Risk Yönetimi Olgunluk Seviyesi ORYOS Endeksi”*** oluşturulmuştur.

4.1. Çalışmanın Aşamaları ve Amacı

Operasyonel risk yönetiminde bankaların genel durumunu ölçmeye yönelik olarak yapılan çalışma aşağıda belirtilen aşamalardan oluşmaktadır;

a) Bankalara gönderilecek ankette yer alan değerlendirme cümlelerinin olgunluk seviye modeline göre hazırlanması,

b) Anketin her bir ana bölümü (insan – sistem –süreç –dışsal etkenler) altında yer alan alt faktörlerin kendi içerisinde AHS yöntemine göre göreli önem derecelerinin belli bir tutarlılık seviyesinde belirlenmesi,

c) Anketin cevaplanmak üzere bankalara gönderilmesi ve cevapların toplanması,

d) Sektördeki her banka için olgunluk seviye modeline göre bir operasyonel risk yönetim olgunluk seviyesi belirlenmesi,

e) Belirlenen olgunluk seviyelerinin AHS yönetimiyle bulunan faktör ağırlıkları ile ağırlıklandırılarak her bir banka için ağırlıklı operasyonel risk yönetim olgunluk seviyesi (ORYOS) hesaplanması,

f) ORYOS'un belli dönemlerde aynı kriterlerle tekrar ölçülmesi ile gerek sektör için gerek banka grupları için (sahiplik, faaliyet açısından)gerekse de münferit olarak her banka için bir operasyonel risk yönetimi olgunluk seviyesi (ORYOS) endeksi hesaplanması.

4.1.1. Anketin Hazırlanması

Bankaların operasyonel risk yönetimi olgunluk seviyelerini ölçmeye yönelik olarak hazırlanacak anket formunda yer alacak soruların neler olması gerektiği konusunda literatür taraması yapılmış ve sektörde risk yönetimi konusunda danışmanlık, eğitim veren konunun uzmanı kişi ve kuruluşların görüş ve değerlendirmelerine başvurulmuştur.

Anketin temelde operasyonel riskin oluşmasına sebebiyet veren insan, sistem, süreç ve dışsal etkenlerden oluşan dört ana faktörden oluşturulması kararlaştırılmıştır. Bu

dört ana bölümün her biri ile doğrudan ilişkili olmayan alt faktörlerde bu bölümlerden hangisine en yakın bulunmuşsa o bölüm içerisinde değerlendirilmiştir.

Anketin hazırlanmasına ilişkin bir sonraki aşamada ise yukarıda bahsi geçen dört ana bölümün (insan, sistem, süreç, dışsal faktörler) her biri için operasyonel risk yönetimine ilişkin sorular belirlenmiştir.

4.1.2. Anketin Bankalara Gönderilmesi ve Ankete Katılım Yüzdesi

Çalışmanın amacı Türk bankacılık sektörü için operasyonel risk yönetimine ilişkin genel bir olgunluk seviyesi belirlemek ve bunun akabinde gerek sektörel gerekse de münferit olarak her banka veya sahiplik, faaliyet türü açısından benzer olan gruplar için operasyonel risk yönetim olgunluk seviyesi hesaplamak olduğu için anket Türkiye Cumhuriyet Merkez Bankası hariç Türkiye'de faaliyet gösteren tüm bankalara istisnasız gönderilmiştir.

Sektörde faaliyet gösteren bankalar sahiplik açısından incelendiğinde, banka türleri; kamu, yerel özel ve yabancı bankalar olmak üzere üç grupta toplanmaktadır. Bu sınıflandırma, banka sermayelerinin ortaklık payları dikkate alınarak yapılmıştır. Yabancı sermaye paylarına, hisseleri Borsada işlem gören bankaların borsadaki halka açıklık oranları dahil edilmiştir. Toplamda borsadaki halka açıklık oranı ve yabancı sermaye ortaklığı %50'den fazla olan bankalar "yabancı banka" statüsünde değerlendirilmiştir. Sermayesinin %50'sinden fazlası yerel gerçek/tüzel kişiye ait olan bankalar "yerel özel banka" statüsünde değerlendirilmiştir. Kalan son grup ise sermayesi büyük ölçüde kamuya ait olan bankalardır ki bunlarda "kamu bankaları" altında sınıflandırılmışlardır. Yapılan bu sınıflandırma gerek BDDK'nın yayımladığı raporlar[262] gerekse de Türkiye Bankalar Birliği[263] ve BDDK'nın internet sitesinde yayımladığı raporlarla teyit edilmiştir[264].

[262] **BDDK Finansal Piyasalar Raporu**, Sayı.12, Aralık 2008, s.21. http://www.bddk.org.tr/WebSitesi/turkce/Raporlar/Finansal_Piyasalar_Raporlari/6320Finansal_Piyasalar_Raporu_Aralik_2008.pdf (12 Mart 2009).
[263] http://www.tbb.org.tr (24 Mayıs 2009).
[264] **BDDK Aylık Bülten**, Mayıs 2009, http://www.bddk.org.tr/WebSitesi/turkce/Istatistiki_Veriler/Aylik_Raporlar/6426Aylik_Bulten_Mayis2009.pdf (13 Haziran 2009) s.3.

Sektörde bulunan bankalar faaliyet açısından üç sınıfa ayrılmaktadır. Bunlar; mevduat, kalkınma ve yatırım ve katılım bankalarıdır. Bankaların sahiplik ve faaliyet açısından sahip oldukları gruplar ve aktif büyüklükleri ile ankete katılım oranlarına ilişkin istatistikler Tablo 31 ve bu tabloyu takip eden grafiklerde yer almaktadır. Toplam 49 bankadan 42'sinin ankete cevap verdiği Tablo 31'de görülmektedir. Ankete katılım yüzdesi banka sayısı açısından %86 olup ankete katılan bankaların aktif büyüklüğü toplamı sektörün toplam aktif büyüklüğünün %99'unu temsil etmektedir.

Tablo 31: Sahiplik, Faaliyet Türü ve Aktif Büyüklüğü Açısından Sektördeki Bankalar ve Ankete Katılım Oranları

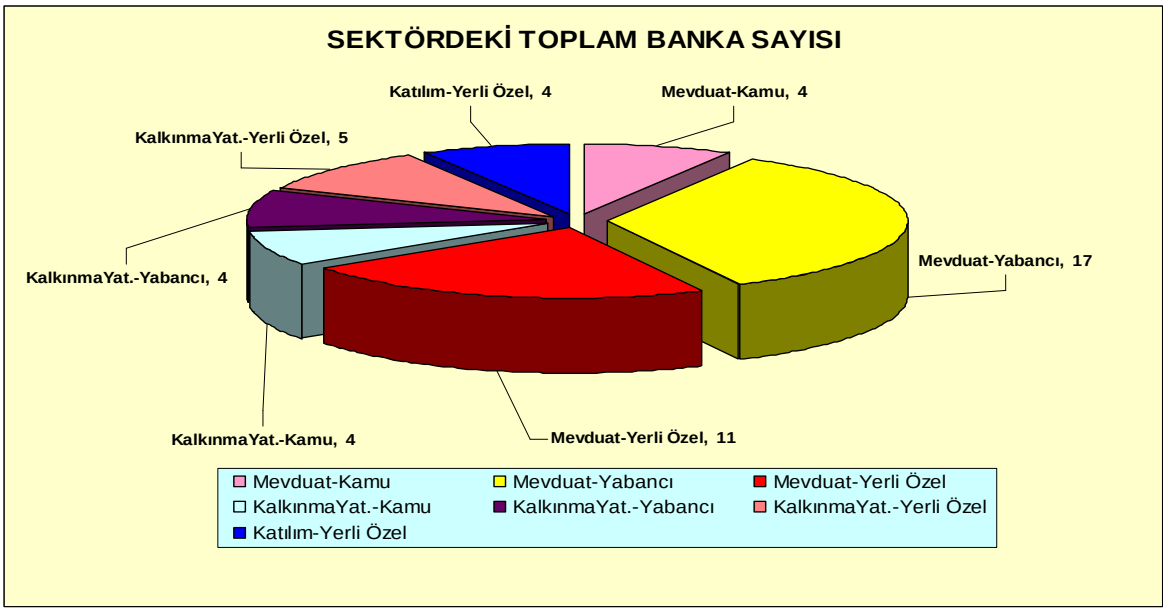
ÇEŞİTLİ İSTATİSTİKLER	BANKALAR TOPLAMI	MEVDUAT			KALKINMA VE YATIRIM			KATILIM
		KAMU	YABANCI	YERLİ ÖZEL	KAMU	YABANCI	YERLİ ÖZEL	YERLİ ÖZEL
TOPLAM BANKA SAYISI	49	4	17	11	4	4	5	4
ANKETE KATILAN BANKA SAYISI	42	3	15	9	4	3	4	4
ANKETE KATILIM YÜZDESİ (%)	86	75	88	82	100	75	80	100
AKTİF BÜYÜKLÜĞÜ (Milyon TL)	678,853	190,792	97,486	345,774	13,816	1,776	5,756	23,454
KATILANLARIN AKTİF TOPLAMI (Milyon TL)	674,967	190,005	95,350	344,996	13,816	1,748	5,599	23,454
AKTİFLERE GÖRE KATILIM YÜZDESİ (%)	99	100	98	100	100	98	97	100

Kaynak: BDDK Aylık Bülten, Mayıs 2009, s.21. BDKK Finansal Piyasalar Raporu, sayı 12, Aralık 2008, s.21. http://www.bddk.org.tr, http://www.tbb.org.tr, http://www.tkbb.org.tr/

Anket içerik itibariyle incelendiğinde, bunu cevaplamaya muhatap personelin bankanın genel uygulamalarına vakıf kişilerden olmasına özen gösterilmiştir. Özellikle bankaların operasyonel risk yönetimi birimlerinde yönetici konumundaki personelin anketi yanıtlamaları talep edilmiştir. Bazı bankalar anketi, insan kaynakları, bilgi işlem, iç kontrol ve iç denetim birimleri ile paylaşarak yanıtladıklarını beyan etmişlerdir.

Sahiplik ve faaliyet açısından sektördeki bankalar ve sayıları Grafik 1'de ayrıca gösterilmektedir.

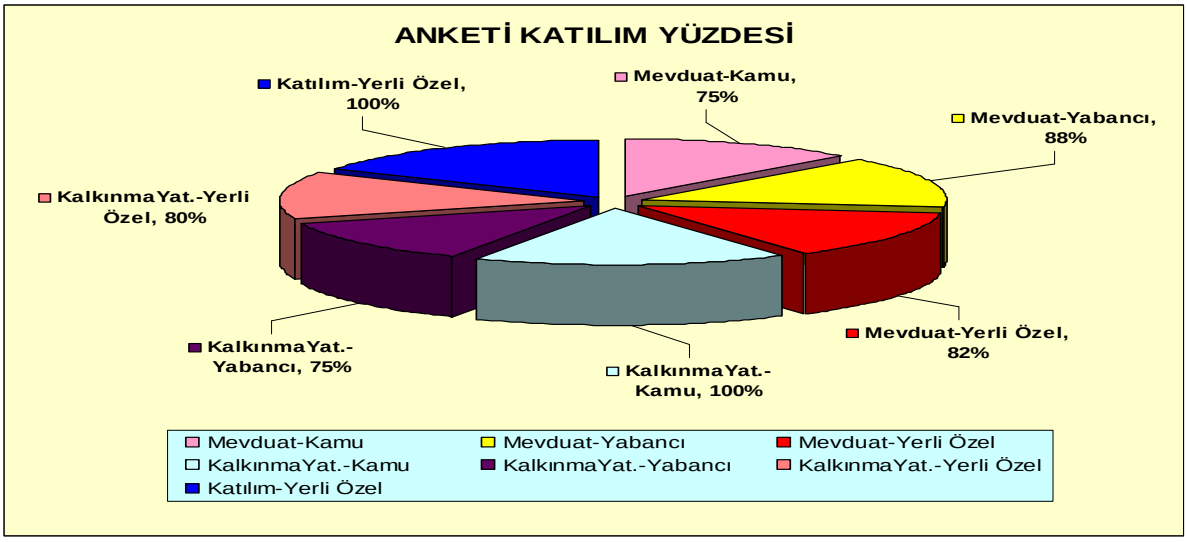
Grafik 1: Sektördeki Bankaların Sahiplik ve Faaliyet Açısından Dağılımı



Kaynak: BDDK Aylık Bülten, Mayıs 2009, s.21. BDKK Finansal Piyasalar Raporu, sayı 12, Aralık 2008, s.21. http://www.bddk.org.tr, http://www.tbb.org.tr, http://www.tkbb.org.tr/

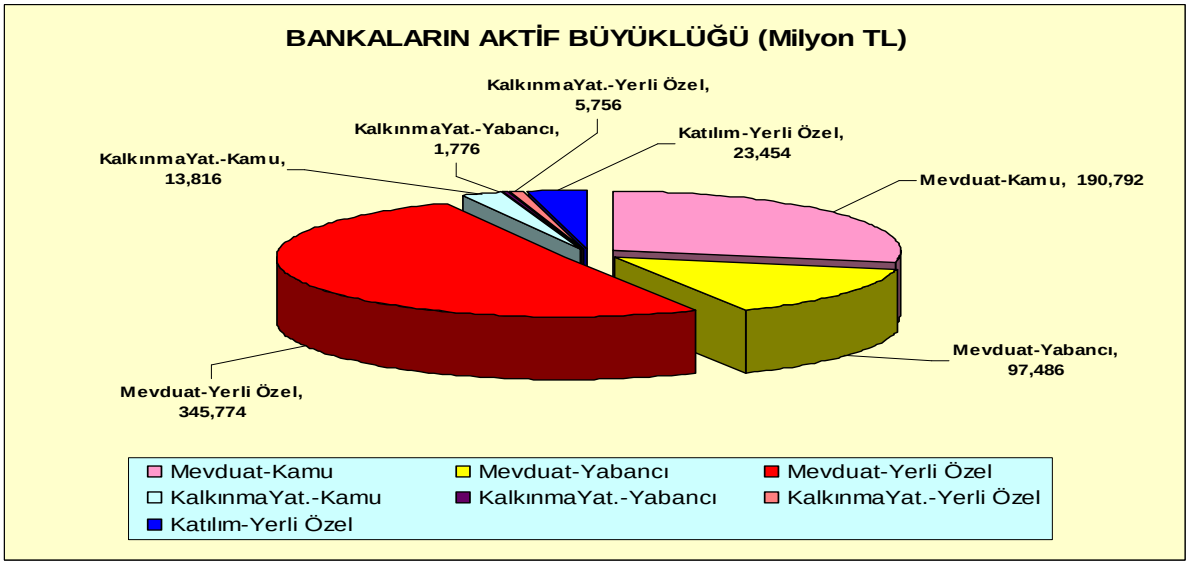
Grafik 2'de bankaların ankete katılım yüzdeleri gösterilmiştir. Buna göre katılım bankaları ile kamuya ait kalkınma ve yatırım bankalarının tamamı ankete katılmıştır. Kamu mevduat bankaları %75, yerli özel sermayeli mevduat bankaları %82, yabancı mevduat bankaları %88, yerli özel kalkınma ve yatırım bankaları %80 ve yabancı sermayeli kalkınma ve yatırım bankaları %75 oranında ankete katılmışlardır.

Grafik 2: Sahiplik ve Faaliyet Türlerine Göre Bankaların Ankete Katılım Oranları



Grafik 3'de sahiplik ve faaliyet açısından banka türlerine ait aktif büyüklükleri yer almaktadır.

Grafik 3: Faaliyet ve Sahiplik Açısından Sektördeki Bankaların Aktif Büyüklükleri



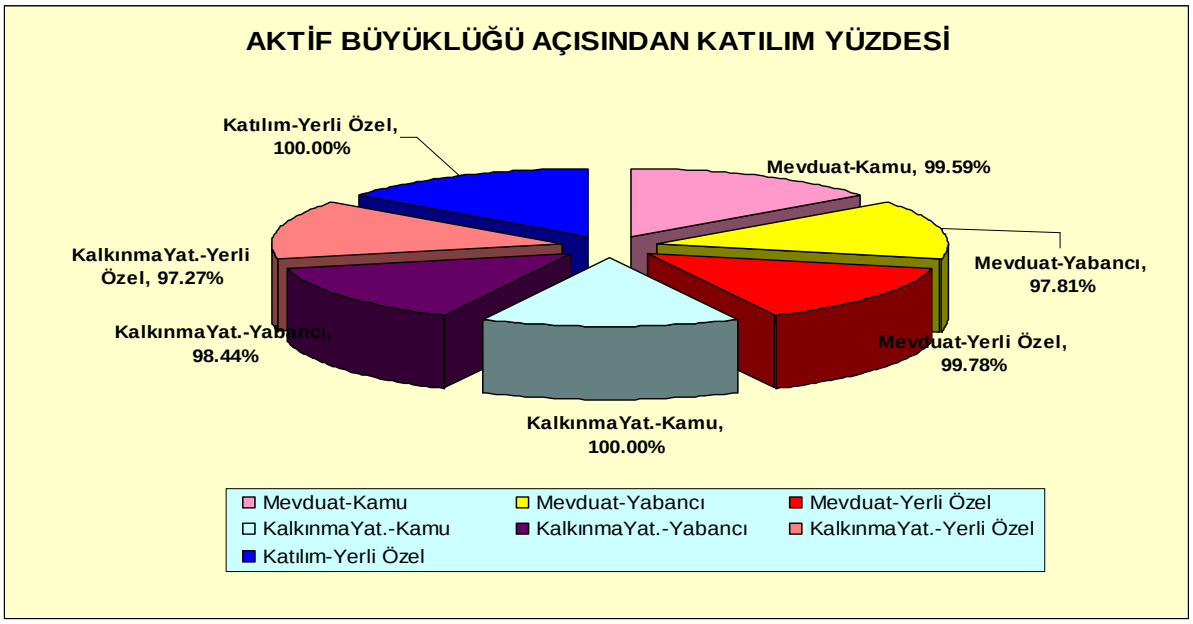
Bankacılık sektörünün toplam aktif büyüklüğü 678,853 Milyon TL'dir. Yerli özel mevduat bankaları 345,774 Milyon TL'lik aktif büyüklüğü ile sektörün %51'ini temsil ederken, kamu mevduat bankaları 190,792 Milyon TL'lik aktif büyüklüğü ile sektörün

%28'lik kısmını, yabancı mevduat bankaları ise 97,486 Milyon TL'lik aktif büyüklüğü ile sektörün %14'ünü temsil etmektedir. Mevduat bankalarının tamamı 634,052 Milyon TL'lik aktif büyüklüğü ile sektörün %93'ünü temsil etmektedir.

Kalkınma ve yatırım bankaları 21,347 Milyon TL'lik aktif toplamı ile sektörün %3'ünü temsil ederken katılım bankalarının aktif toplamı 23,454 Milyon TL ve temsil yüzdesi %3 civarındadır.

Grafik 4'de ankete katılan bankaların sahiplik ve faaliyet türü bazında aktif büyüklükleri açısından ankete katılım yüzdeleri verilmiştir. Ankete katılan bankaların aktif toplamları sektörün aktif toplamının %99'una isabet etmektedir ki bu oran katılımın fevkalade yüksek olduğunu göstermektedir.

Grafik 4: Ankete Katılan Bankaların Aktif Büyüklükleri



4.1.3. Sonuçların Analizi ve ORYOS Puanlarının Ağırlıklandırılması

"İnsan", "Sistem", "Süreç" ve "Dışsal Etkenler" olmak üzere dört ana bölümden oluşan ankete bankalarca verilen cevaplar münferit olarak banka bazında değerlendirmeye tabi tutulmasına rağmen çalışmada söz konusu bankalar sahiplik ve faaliyet türüne göre oluşturulan gruplara göre analiz edilmiştir.

Ankette, bankalardan dört ana bölümden (insan, sistem, süreç, dışsal faktörler)oluşan toplam 33 adet cümleyi değerlendirmesi istenmiştir. Dört ana faktör içinde yer alan 33 adet değerlendirme cümlesinin her birinin altında olgunluk seviyesi sıfır (0-varolmayan) ile beş (5-Optimize edilmiş) arasında değişen 6 farklı seviyede cümle yer almıştır. Bankalardan istenen 33 adet değerlendirme cümlesinin her biri için altlarında yer alan 6 farklı seviyedeki cümlelerden kendi durumlarını en iyi yansıtan cümleyi seçmek olmuştur ki seçilen cümlelerin her biri bir olgunluk seviyesine karşılık gelmektedir.

Sonuçta her banka için dört ana faktör altında yer alan 33 adet alt faktör için 0 ile 5 arasında olgunluk seviye puanı tespit edilmiştir. Bu puanlar AHS yöntemiyle belirlenmiş her bir ana faktör altındaki alt faktörlerin göreli önem dereceleriyle ağırlıklandırılmıştır.

Her bir ana faktör altındaki alt faktör grupları için hesaplanan puanlar toplanarak ilgili ana faktör grubunun AHS ile ağırlıklandırılmış olgunluk seviyesi belirlenmiştir. Yani sonuçta bir bankanın dört ana faktör için hesaplanmış dört tane olgunluk seviye puanına ulaşılmıştır. Bu dört ana faktörün aritmetik ortalaması alınarak bankanın AHS ile ağırlıklandırılmış genel olgunluk seviye puanına ulaşılmıştır.

4.1.4. Sahiplik Açısından Bankaların ORYOS Puanlarının Değerlendirilmesi

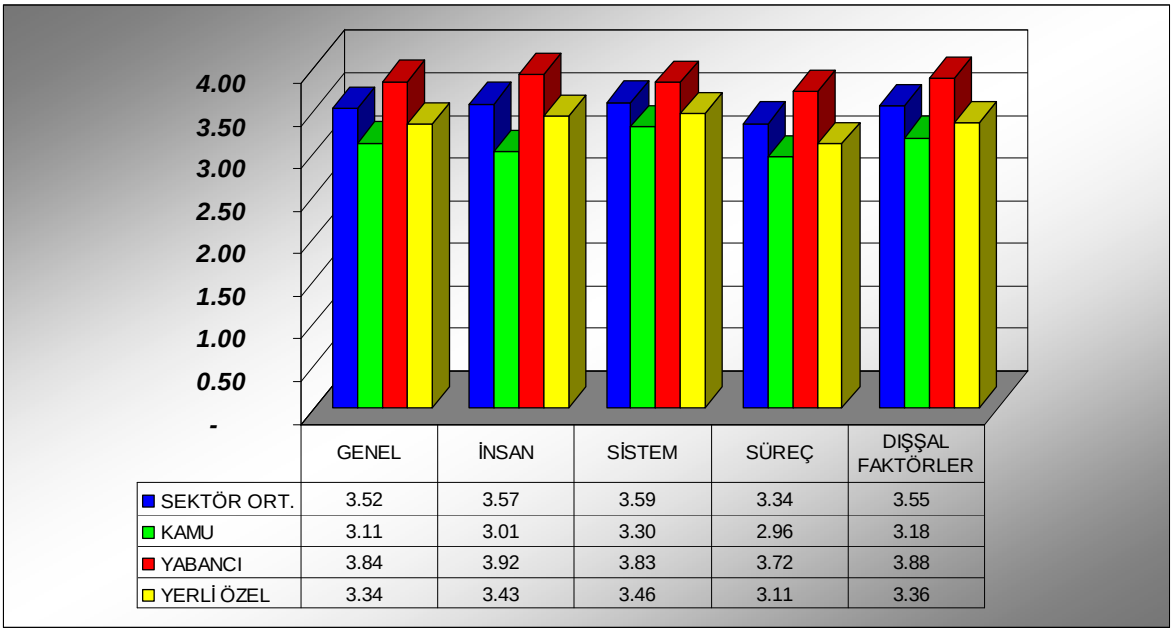
Sahiplik açısından bankalar kamu, yerel özel ve yabancı banka olmak üzere üç gruba ayrılmıştır. Her grubun her bir ana faktör içinde (insan, sistem, süreç, dışsal etkenler) aldığı ağırlıklı olgunluk seviye puanlarının aritmetik ortalaması alınarak ilgili ana faktöre ait banka grubunun (kamu, yerel özel, yabancı) AHS ile ağırlıklandırılmış ortalama olgunluk seviye puanı hesaplanmıştır.

Dört ana faktör bazında tüm bankalar dahil edilerek bulunan aritmetik ortalama ile de her bir ana faktör için sektör ortalamasına ulaşılmıştır. Her bir bankanın genel puanlarının aritmetik ortalaması alınarak da bankacılık sektörünün operasyonel risk yönetim olgunluk seviyesine ulaşılmıştır.

Grafik 5 incelendiğinde operasyonel risk yönetimine ilişkin sektörün genel olgunluk seviyesi puanı 5 üzerinden 3.52 bulunmuştur. Sektör ortalamasının dört ana faktör arasındaki dağılımı da 3.34 (süreç) ile 3.59 (sistem) arasında değişmektedir.

Sektörün yabancı banka grubuna ait ortalaması 3.84 ile hem sektör ortalamasının üzerinde hem de kamu ve yerel özel bankaların sektör ortalamasının üzerindedir. Dört ana faktör için de yabancı bankaların ortalama olgunluk seviye puanları değerlendirildiğinde kamu ve yerel özel bankalar göre en üst seviyede oldukları görülmektedir. Sahiplik açısından banka türleri arasında bulunan kamu bankalarının ortalama genel olgunluk seviyesinin hem sektörün genel ortalaması hem de operasyonel risk yönetiminin dört temel alanı için (insan, sistem, süreç, dışsal etkenler) en alt seviyede oldukları dikkat çekmektedir.

Grafik 5: Sahiplik Türleri Bazında Bankaların Operasyonel Risk Yönetim Faktörlerinden Aldıkları Ağırlıklı Puanlar ve Sektör Ortalaması ile Karşılaştırma



	GENEL	İNSAN	SİSTEM	SÜREÇ	DIŞSAL FAKTÖRLER
SEKTÖR ORT.	3.52	3.57	3.59	3.34	3.55
KAMU	3.11	3.01	3.30	2.96	3.18
YABANCI	3.84	3.92	3.83	3.72	3.88
YERLİ ÖZEL	3.34	3.43	3.46	3.11	3.36

Sonuç olarak bankacılık sistemimizde faaliyet gösteren yabancı bankaların operasyonel risk yönetimi genel olgunluk seviyesi yerel özel ve kamu bankalarına göre daha iyi durumdadır. Bu sıralamada yerel özel bankaların olgunluk seviyesi orta düzeyde yer alırken kamu bankaları sıralamada son sırada bulunmaktadır. Bu sıralama operasyonel risk yönetiminin dört ana unsuru için de ayrı ayrı yapıldığında sonuç yine değişmemektedir.

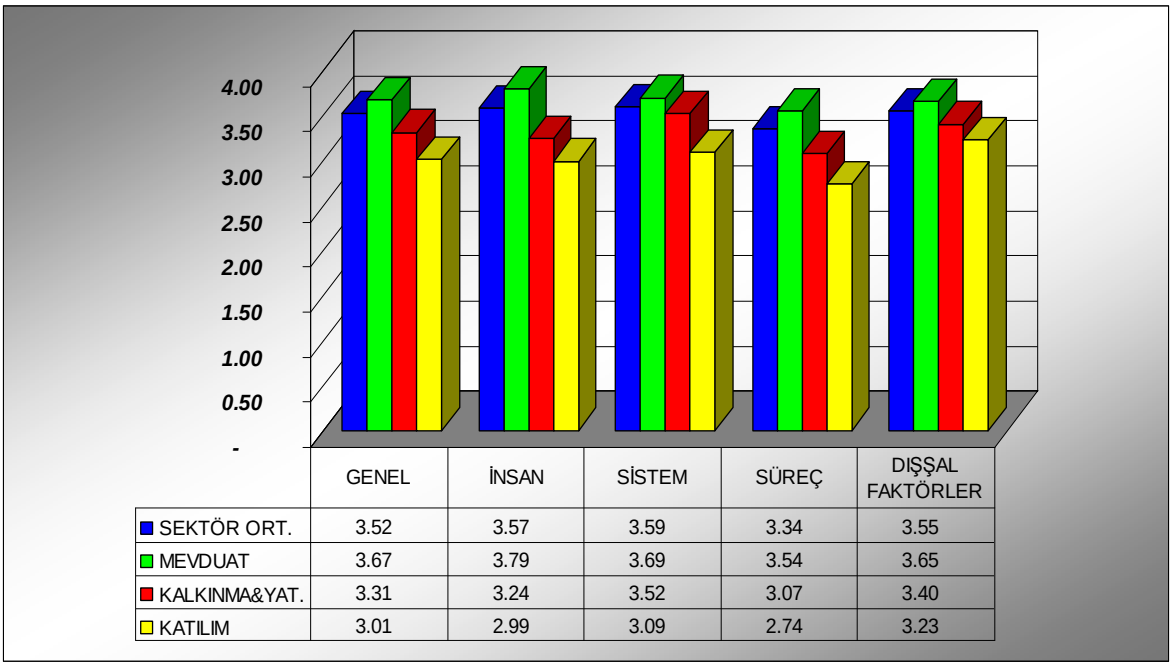
4.1.5. Faaliyet Açısından Bankaların ORYOS Puanlarının Değerlendirilmesi

Faaliyet açısından bankalar mevduat, kalkınma ve yatırım ve katılım bankaları olmak üzere üç gruba ayrılmıştır. Her grubun her bir ana faktör içinde (insan, sistem, süreç, dışsal etkenler) aldığı ağırlıklı olgunluk seviye puanlarının aritmetik ortalaması alınarak ilgili ana faktöre ait banka grubunun (mevduat, kalkınma ve yatırım, katılım) AHS ile ağırlıklandırılmış ortalama olgunluk seviye puanı hesaplanmıştır.

Sektörün genel olgunluk seviyesi puanı ile dört ana faktörün olgunluk seviye puanları sahiplik açısından banka türleri için yapılan analizde bulunmuştu.

Grafik 6'da faaliyet türlerine göre gruplanan bankaların operasyonel risk yönetiminin dört ana faktörü için hesaplanmış ortalama olgunluk seviyeleri ile bu dört faktörün aritmetik ortalamasından elde edilen genel olgunluk seviyeleri bulunmuş ve bunlar sektör ortalamaları ile karşılaştırılmıştır.

Grafik 6: Faaliyet Türleri Bazında Bankaların Operasyonel Risk Yönetim Faktörlerinden Aldıkları Ağırlıklı Puanlar ve Sektör Ortalaması ile Karşılaştırma



	GENEL	İNSAN	SİSTEM	SÜREÇ	DIŞSAL FAKTÖRLER
SEKTÖR ORT.	3.52	3.57	3.59	3.34	3.55
MEVDUAT	3.67	3.79	3.69	3.54	3.65
KALKINMA&YAT.	3.31	3.24	3.52	3.07	3.40
KATILIM	3.01	2.99	3.09	2.74	3.23

Sektördeki mevduat bankalarının dört ana faktörden her biri için bulunan ortalama olgunluk seviyesi ile dört faktörün aritmetik ortalaması alınarak hesaplanan genel olgunluk seviyesi hem sektör ortalamasının hem de sektörde faaliyet gösteren kalkınma ve yatırım bankaları ve katılım bankalarının olgunluk seviyesinden yüksektir. Olgunluk seviyesinde sektör genel ortalaması 3.52 iken mevduat bankalarının ki 3.67, kalkınma ve yatırım bankalarının ki 3.31 ve katılım bankalarının ki 3.01'dir. Dört ana faktör karşılaştırması yapıldığında da mevduat bankalarının olgunluk seviyesi en üstte yer almaktadır. Örneğin olgunluk seviyesi mevduat bankalarında "İnsan" faktörü için 3.79, "Sistem" faktörü için 3.69, "süreç" faktörü için 3.54 ve "dışsal etkenler" faktörü için 3.65 hesaplanmıştır.

Faaliyet açısından diğer banka gruplarına baktığımızda katılım bankaları en alt seviyede bulunurken, kalkınma ve yatırım bankaları bu iki grubun ortasında yer almaktadır.

Sonuç olarak bankacılık sistemimizde faaliyet gösteren mevduat bankalarının operasyonel risk yönetimi genel olgunluk seviyesi kalkınma ve yatırım ve katılım bankalarına göre daha iyi durumdadır. Bu sıralamada kalkınma ve yatırım bankalarının olgunluk seviyesi orta düzeyde yer alırken katılım bankaları sıralamada son sırada bulunmaktadır.

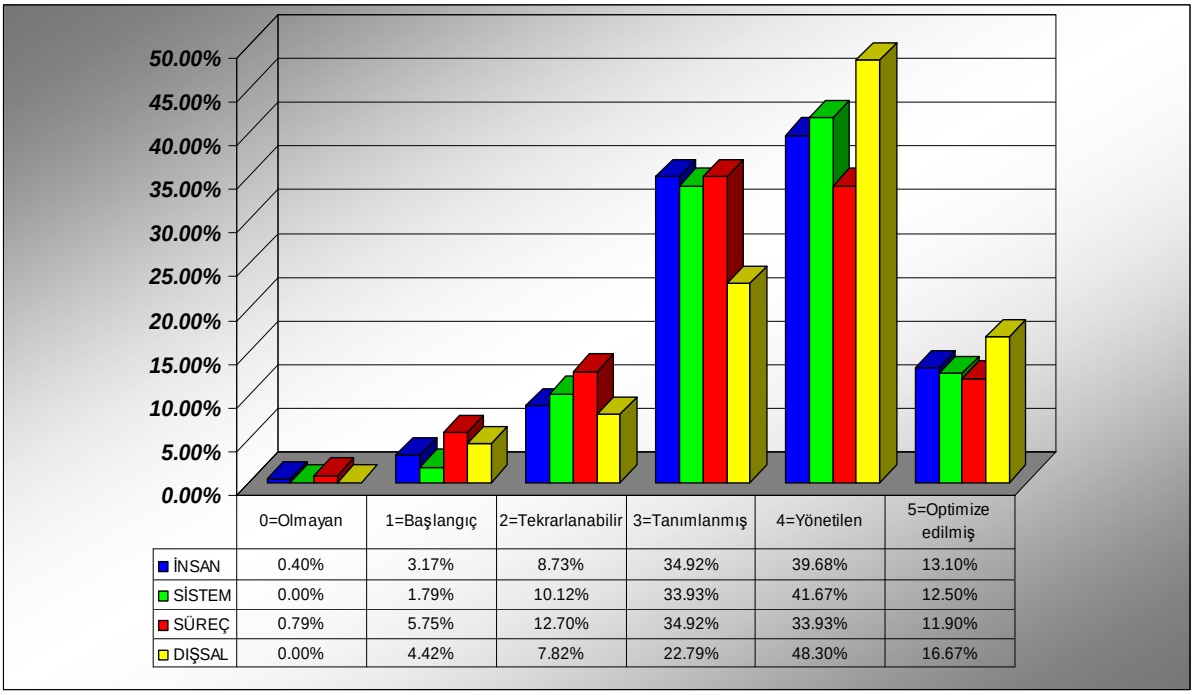
4.1.6. Anket Sonuçlarının Sektörel ve Dört Ana faktör Bazında Analizi

Bankaların ankete verdikleri yanıtlar AHS yöntemi ile ağırlıklandırılmadan analiz edildiğinde operasyonel risk yönetiminde sektörün her bir faktör için ne derecede hangi olgunluk seviyesinde olduğu bilgisine ulaşılmaktadır.

Grafik 7'nin hazırlanmasında öncelikle tüm bankaların ankette dört ana faktör için 0 ila 5 arasında belirttikleri olgunluk seviyeleri faktörler bazında sayılmıştır. Yani örneğin "İnsan" faktörü altında yer alan 6 adet alt faktör için bankaların her bir olgunluk seviyesinden kaç adet seçtikleri sayılmıştır. Bu sayım diğer ana faktörler için "Sistem", "Süreç" ve "Dışsal Etkenler" için de tekrarlanmıştır. Her bir ana faktör altında yer alan her bir olgunluk seviyesine düşen sayılar listelenmiş ve her bir olgunluk seviyesinin ilgili faktör içindeki yüzdesel payı bulunmuştur.

Grafik 7 incelendiğinde insan faktörü için sektörün operasyonel risk yönetimi olgunluk seviyesinin %34.92 oranında 3 seviyesinde, %39,68 oranında 4 seviyesinde ağırlıklı olarak toplandığı görülmektedir. Sistem faktörü için sektörün olgunluk seviye dağılımına bakıldığında ortalama %75 civarında 3 ila 4 olgunluk seviyesinde dağıldığı görülmüştür. Süreç faktörü için dağılıma bakıldığında 3 ila 4 olgunluk seviyesinin her biri için ortalama %34'lük bir paya sahip olduğu, 2 ve 5 olgunluk seviyeleri için de %12'şerlik paylara sahip oldukları görülmüştür. Dışsal etkenlerin grafiğe yansıması analiz edildiğinde, bu faktöre ilişkin operasyonel risklerin neredeyse %50 civarında 4 (yönetilen) olgunluk seviyesinde olduğu görülmüştür.

Grafik 7: Sektörün Operasyonel Risk Yönetimine İlişkin Dört Ana Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı



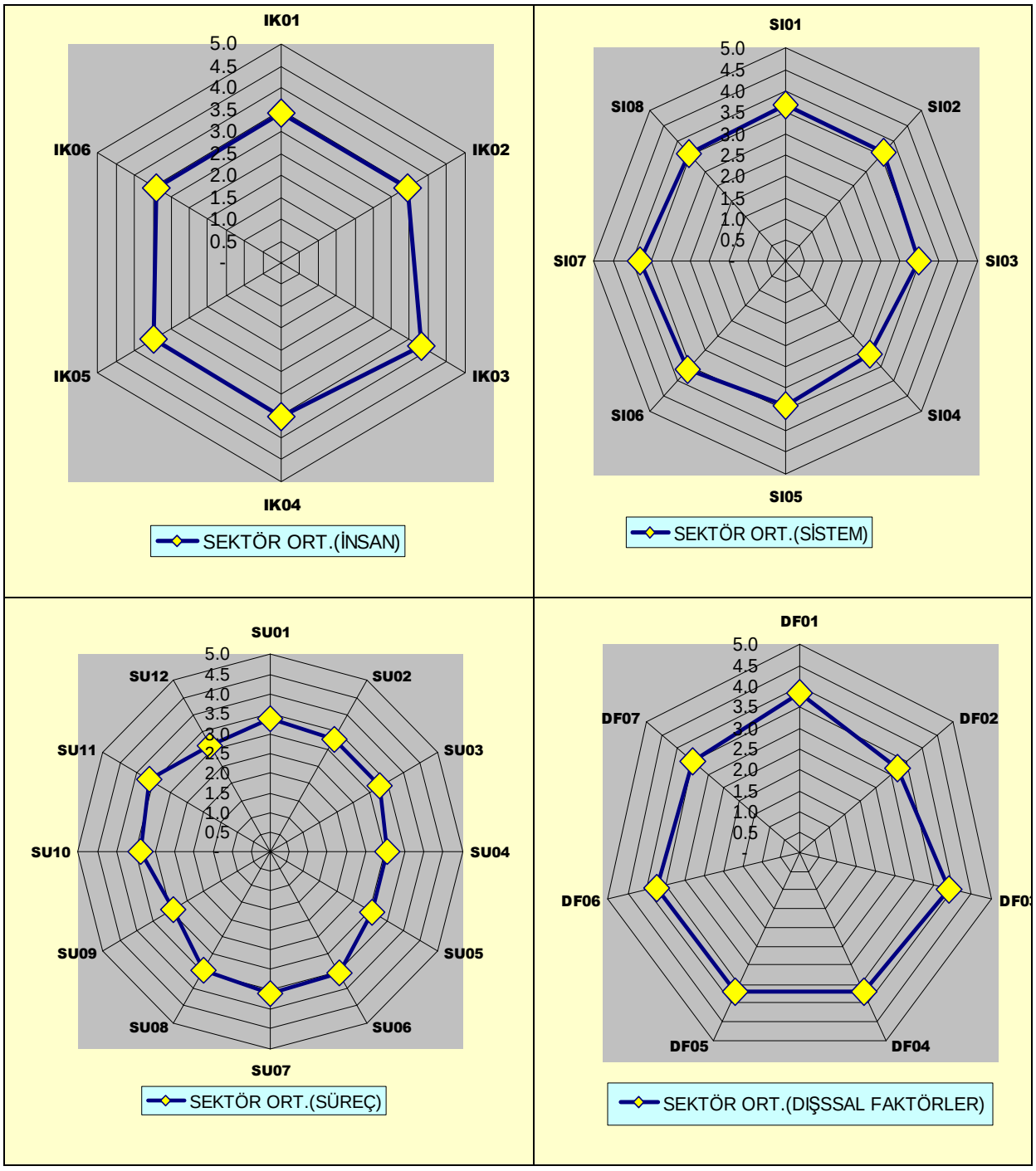
	0=Olmayan	1=Başlangıç	2=Tekrarlanabilir	3=Tanımlanmış	4=Yönetilen	5=Optimize edilmiş
İNSAN	0.40%	3.17%	8.73%	34.92%	39.68%	13.10%
SİSTEM	0.00%	1.79%	10.12%	33.93%	41.67%	12.50%
SÜREÇ	0.79%	5.75%	12.70%	34.92%	33.93%	11.90%
DIŞSAL	0.00%	4.42%	7.82%	22.79%	48.30%	16.67%

Ana faktörlere ait her bir alt faktörün ortalama olgunluk seviyesinin, sahiplik veya faaliyet türü açısından diğer banka gruplarının olgunluk seviyeleri ile karşılaştırması için en uygun grafik örümcek ağı türü grafiklerdir.

Grafik 8 dört bölümden oluşmaktadır. Her bir bölüm ankette yer alan dört ana faktörden (insan, sistem, süreç, dışsal faktörler) birini temsil etmektedir. Sol üst köşedeki

birinci şekil anketteki “İnsan” faktörünü, bu şeklin içerisindeki örümcek ağına benzeyen şekilde bu ana faktör altında bankalara yöneltilen alt faktörlere ait değerlendirme cümlelerini temsil etmektedir. Örneğin “İnsan” faktörü için bankalara, 6 adet değerlendirme cümlesinin her biri için kendilerine en uygun seviyeyi 0 ila 5 olgunluk seviyesi arasında seçmeleri istenmişti. İşte bu şekilde bankaların ilgili alt faktör için seçtikleri olgunluk seviyelerinin sektör ortalaması gösterilmektedir. Örneğin sektördeki bankaların İK01 alt faktörü için ortalama olgunluk seviyesi 3.40’dır. Gerçekten de Grafik 7 incelendiğinde bankaların “İnsan” faktörü için olgunluk seviyelerinin yüzdesel dağılımında yaklaşık %85’lik bir payın 3 ila 4 olgunluk seviyesinde (tam değer 3.40) bulunduğu görülmüştü.

Grafik 8: Dört Ana Faktörü Altında Yer Alan Alt Faktörlerin Olgunluk Seviyelerinin Sektör Ortalamaları

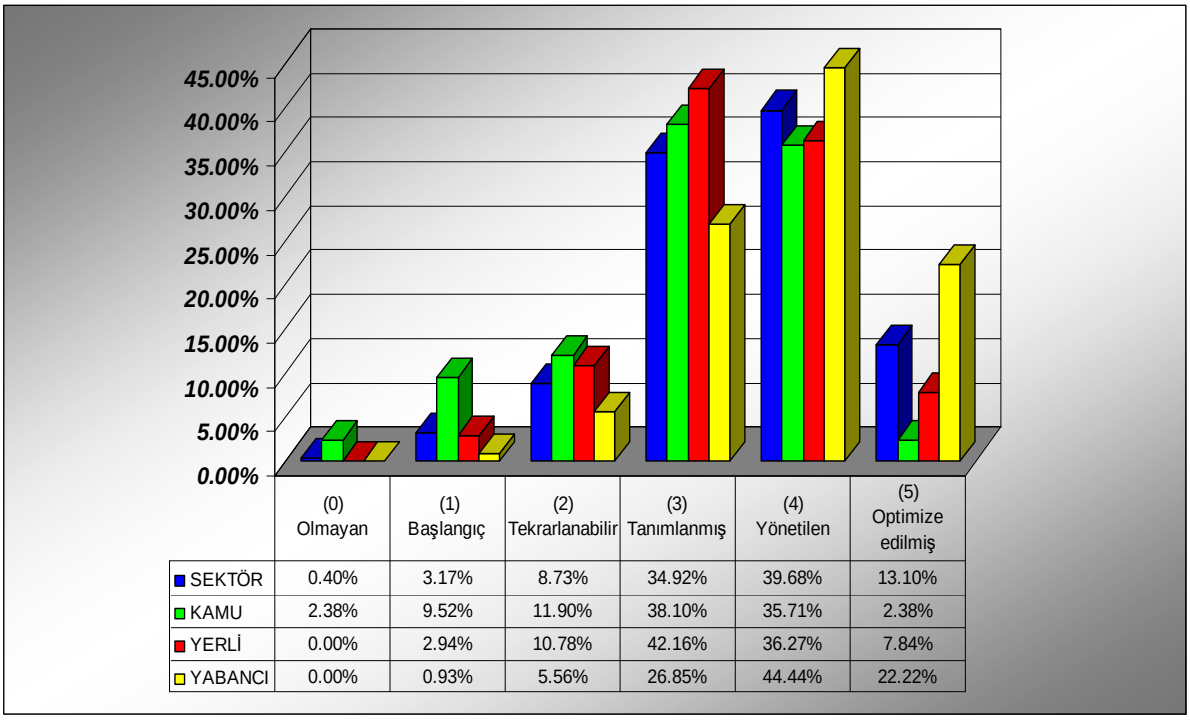


Grafikteki şekiller bankacılık sektörünün dört ana faktörü için ortalama olgunluk seviyelerini mükemmel görsellikte göstermektedir.

4.1.7. Sahiplik Açısından Banka Türlerine Göre Anketin Değerlendirilmesi

Grafik 9'da sahiplik açısından gruplara ayrılan banka türlerinin "insan" faktörü altındaki değerlendirme cümlelerine ilişkin olgunluk seviyelerinin yüzdesel dağılımı gösterilmektedir. Grafik dikkatle incelendiğinde yabancı bankaların insan faktörüne ilişkin olgunluk seviyeleri %27'lik pay ile 3 (tanımlanmış), %44'lük pay ile 4 (yönetilen) ve %22'lik pay ile 5(optimize edilmiş) olarak belirlenmiştir.

Grafik 9:Sahiplik Açısından Banka Türlerinin "İnsan" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması

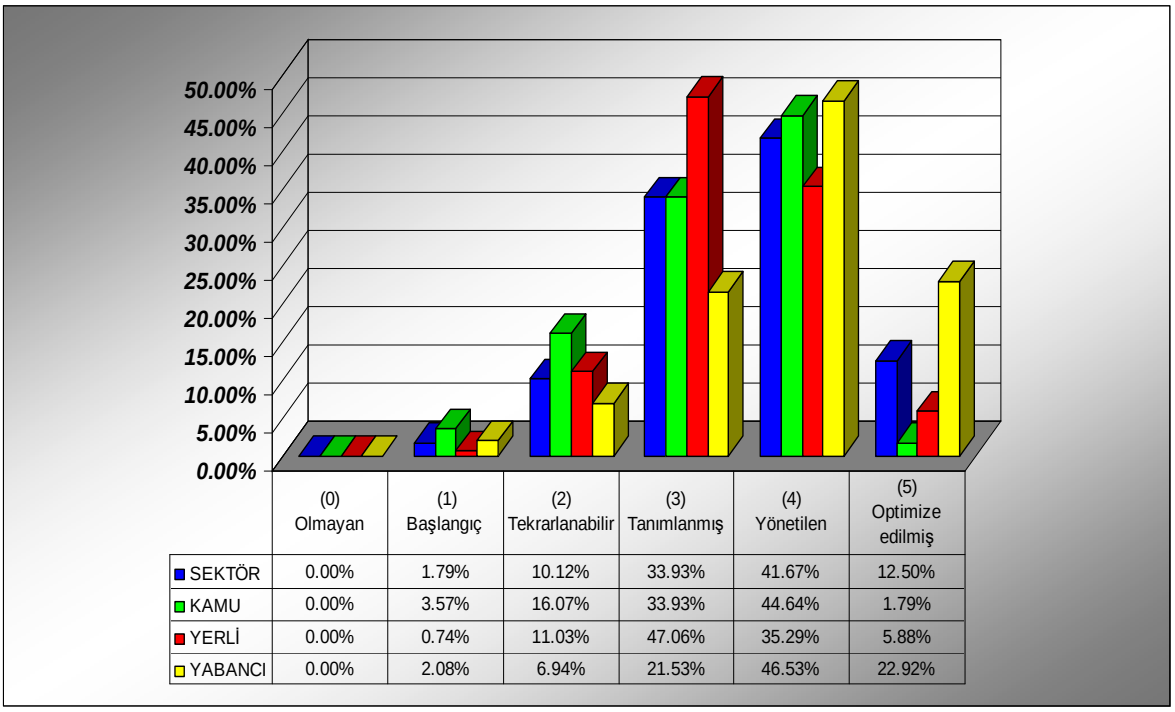


	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.40%	3.17%	8.73%	34.92%	39.68%	13.10%
KAMU	2.38%	9.52%	11.90%	38.10%	35.71%	2.38%
YERLİ	0.00%	2.94%	10.78%	42.16%	36.27%	7.84%
YABANCI	0.00%	0.93%	5.56%	26.85%	44.44%	22.22%

Aynı faktör için kamu bankalarının olgunluk seviyeleri %85'lik kümülatif pay ile 3 ve 4 arasında paylaşılmıştır. Yerli özel bankaların olgunluk seviyesine bakıldığında, %42'lik pay ile 3 (tanımlanmış) ve %36'lık pay ile 4(yönetilen) derecesinde olduğu görülmektedir. Sektör ortalaması da %85'lik pay ile 3 ve 4 olgunluk seviyeleri etrafında toplanmıştır.

Grafik 10, kamu, yerli özel ve yabancı bankalar için “sistem” faktörüne ilişkin olgunluk seviye dağılımlarını yüzdesel olarak göstermektedir. Grafik incelendiğinde yabancı bankaların olgunluk seviyelerinin 3, 4, 5 etrafında bir dağılım yaptığı, kamu ve yerli özel bankaların ise genelde 3 ila 4 etrafında toplandığı görülmektedir. Örneğin yerli özel bankalar “sistem” faktörü için %47 gibi yüksek oranda 3 (tanımlanmış) olgunluk seviyesinde bulunmaktadırlar.

Grafik 10: Sahiplik Açısından Banka Türlerinin “Sistem” Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması

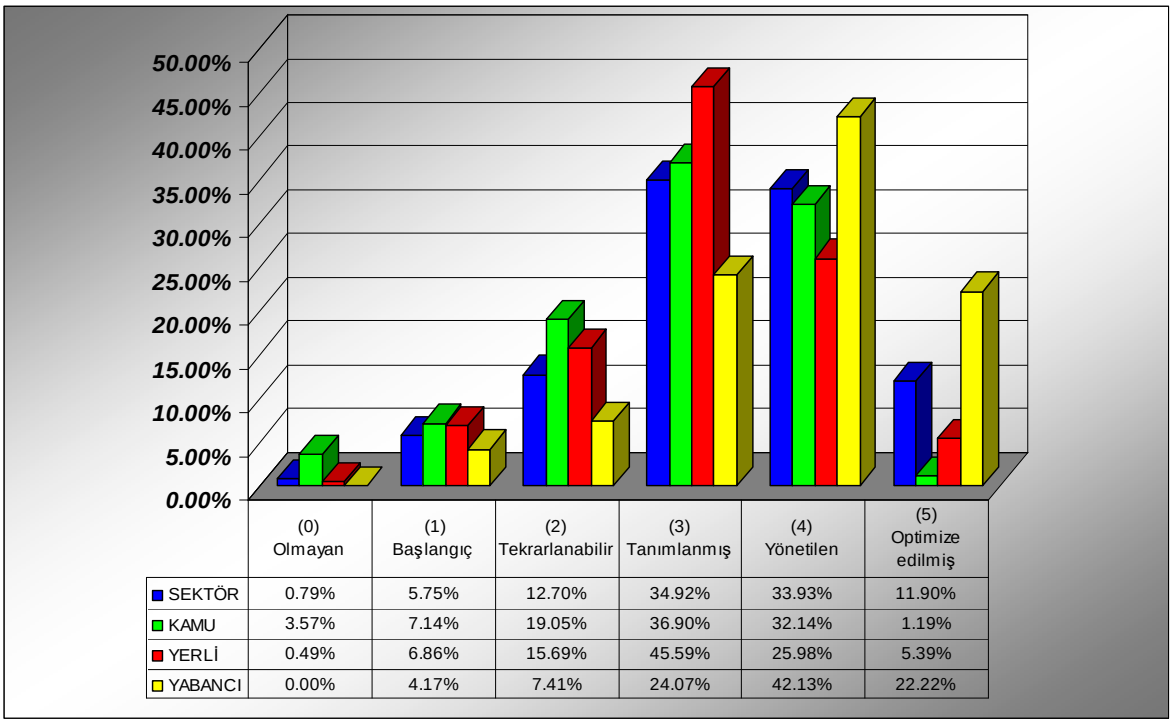


	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.00%	1.79%	10.12%	33.93%	41.67%	12.50%
KAMU	0.00%	3.57%	16.07%	33.93%	44.64%	1.79%
YERLİ	0.00%	0.74%	11.03%	47.06%	35.29%	5.88%
YABANCI	0.00%	2.08%	6.94%	21.53%	46.53%	22.92%

Grafik 11’de aynı banka grubunun “süreç” faktörü için yapılan olgunluk seviye dağılımı gösterilmektedir. Grafikte %46 ile yerli bankaların 3 (tanımlanmış) seviyesinde oldukları dikkat çekmektedir. Yabancı bankaların dağılımı yine ağırlıklı olarak 4 civarında (%42) olmakla beraber, %24’lik pay ile 3, %22’lik pay ile de 5 seviyesinde toplanmıştır. Kamu bankalarının ağırlıklı seviyeleri %70’e varan oranlarda 3-4 civarında toplanmıştır. Kamu ve yerli özel bankaların “süreç” faktörü için belirlenen ortalama olgunluk seviyelerinin

5 seviyesinde çok az olması bu bankaların süreç tasarımlarında, süreçlerden kaynaklanan operasyonel riskleri yönetmede daha kat edecek yolları olduğunu göstermektedir.

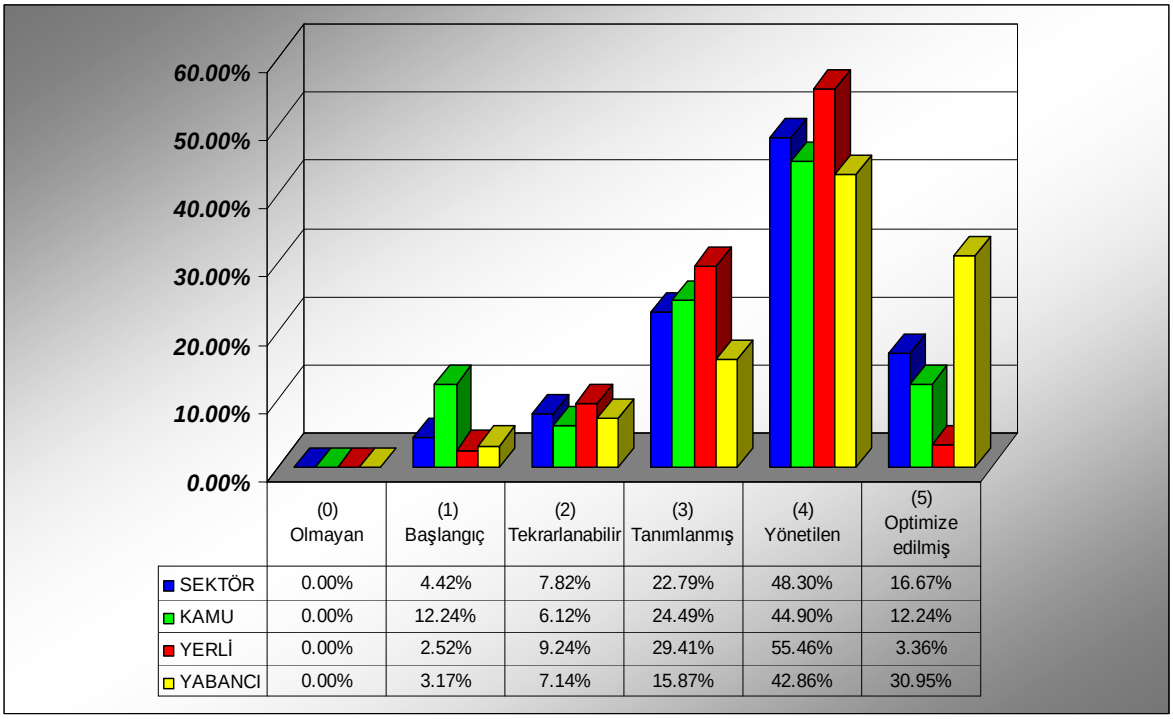
Grafik 11: Sahiplik Açısından Banka Türlerinin "Süreç" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması



	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.79%	5.75%	12.70%	34.92%	33.93%	11.90%
KAMU	3.57%	7.14%	19.05%	36.90%	32.14%	1.19%
YERLİ	0.49%	6.86%	15.69%	45.59%	25.98%	5.39%
YABANCI	0.00%	4.17%	7.41%	24.07%	42.13%	22.22%

"Dışsal etkenler" faktörü için olgunluk seviyeleri Grafik 12'den de görüleceği üzere bu gruptaki tüm banka türleri için büyük ölçüde 4 seviyesinde toplanmış, hatta yabancı banklar için %31'ler seviyesinde 5 civarındadır. Yani bankalar operasyonel riskin bu faktörünü daha ciddiye almışlar ve yönetmektedirler.

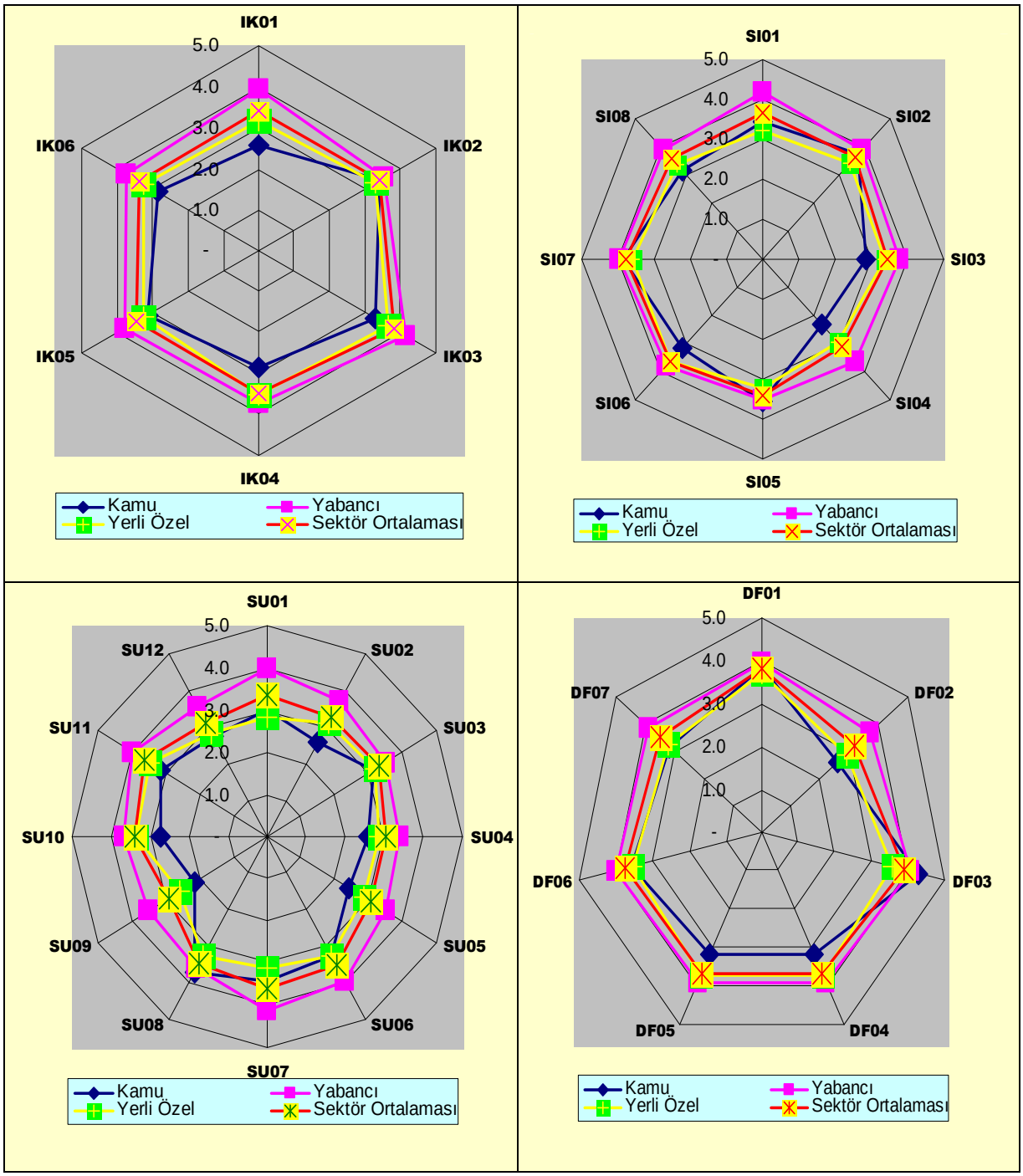
Grafik 12: Sahiplik Açısından Banka Türlerinin "Dışsal Etkenler" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması



	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.00%	4.42%	7.82%	22.79%	48.30%	16.67%
KAMU	0.00%	12.24%	6.12%	24.49%	44.90%	12.24%
YERLİ	0.00%	2.52%	9.24%	29.41%	55.46%	3.36%
YABANCI	0.00%	3.17%	7.14%	15.87%	42.86%	30.95%

Grafik 13'de sahiplik açısından banka türlerinin anketin dört ana faktörü altında yer alan alt faktörler için belirledikleri ortalama olgunluk seviyelerinin dağılımı gösterilmektedir.

Grafik 13: Sahiplik Açısından Banka Türleri İçin Dört Ana Faktör Altındaki Alt Faktörlerin Ortalama Olgunluk Seviyeleri



Örümcek ağı şeklindeki grafiklerle banka türlerinin kendi aralarındaki olgunluk seviyeleri rahatlıkla karşılaştırılabilmektedir. Örneğin yukarıdaki grafikte yer alan şekillerde operasyonel riskin dört faktörü için de kamu bankalarının olgunluk seviye ortalamaları örümcek ağının en içinde yer alırken, yabancı bankaların ağın en dışında yani en yüksek olgunluk seviyesinde bulundukları rahat bir görsellikle sergilenmektedir.

4.1.8. Faaliyet Açısından Banka Türlerine Göre Anketin Değerlendirilmesi

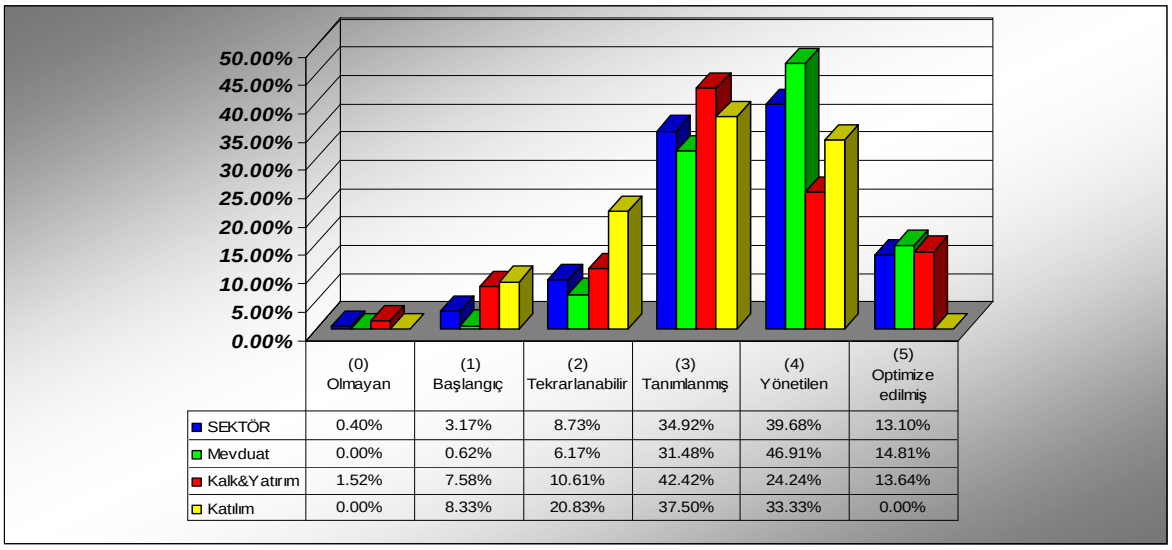
Bu kısımda ankete verilen cevaplar faaliyet açısından gruplanan banka türleri için değerlendirilecektir. Operasyonel riskin dört ana faktörüne ilişkin yönetim uygulamalarına yönelik olarak faaliyet açısından gruplandırılan bankaların olgunluk seviyeleri grafiklerle analiz edilecektir.

Grafik 14'de mevduat, kalkınma ve yatırım ve katılım bankalarının "insan" faktörü altındaki değerlendirme cümlelerine ilişkin olgunluk seviyelerinin yüzdesel dağılımı gösterilmektedir. Grafik incelendiğinde mevduat bankalarının bu faktöre ilişkin olgunluk seviye dağılımının %31 ile 3(tanımlanmış), %47 ile 4(yönetilen) düzeyinde toplandığı görülmektedir ki bu iyi bir seviyedir. Kalkınma ve yatırım bankaları yoğunluklu olarak %42 ile 3 olgunluk seviyesinde, %24 ile 4 olgunluk seviyesinde yer almaktadır. Katılım bankalarının belirttikleri seçeneklere göre olgunluk seviyelerinin yüzdesel dağılımını %21 ile 2, %38 ile 3, %33 ile 4 düzeyinde toplanmıştır.

Sonuç olarak faaliyet açısından banka türleri içinde "insan" faktörüne ilişkin operasyonel risk yönetim seviyesinde mevduat bankalarının durumu gruptaki diğer banka türlerine göre daha yukarıda görülmekte, katılım bankaları sıralamada aşağıda yer almaktadır.

Sektör ortalamasına bakıldığında olgunluk seviye dağılımının yoğunluklu olarak %35 ile 3(tanımlanmış), %40 ile 4(yönetilen) düzeyinde olduğu görülmektedir.

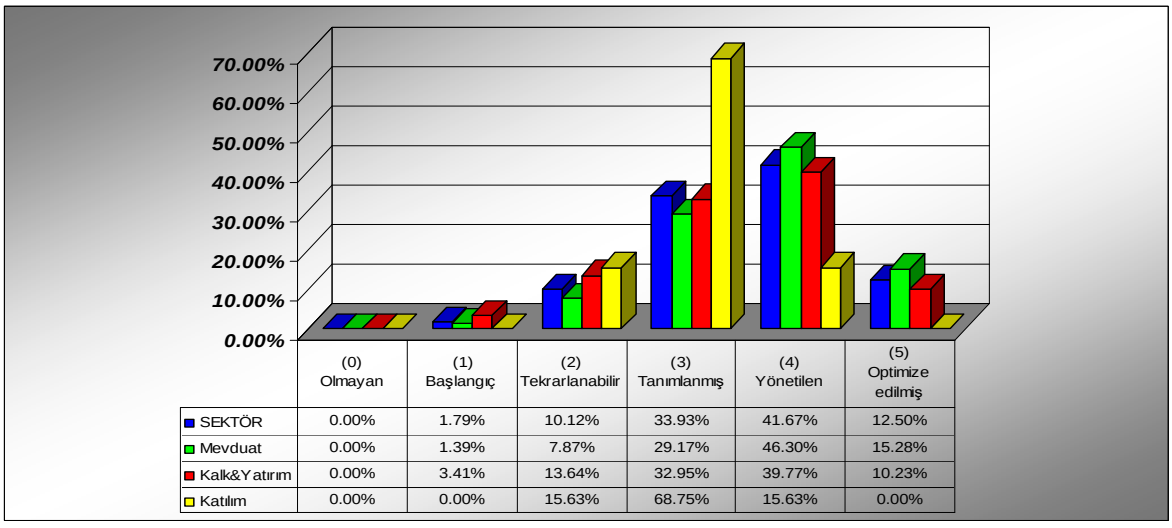
Grafik 14: Faaliyet Açısından Banka Türlerinin "İnsan" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması



	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.40%	3.17%	8.73%	34.92%	39.68%	13.10%
Mevduat	0.00%	0.62%	6.17%	31.48%	46.91%	14.81%
Kalk&Yatırım	1.52%	7.58%	10.61%	42.42%	24.24%	13.64%
Katılım	0.00%	8.33%	20.83%	37.50%	33.33%	0.00%

Sistem faktörüne ilişkin bankaların faaliyet türü bazındaki gruplara ilişkin olgunluk seviyeleri Grafik 15'de incelenmiştir. Katılım bankalarının %69 ile 3 seviyesinde, mevduat bankalarının %29 ile 3, %46 ile 4 seviyesinde oldukları öne çıkan hususlardır.

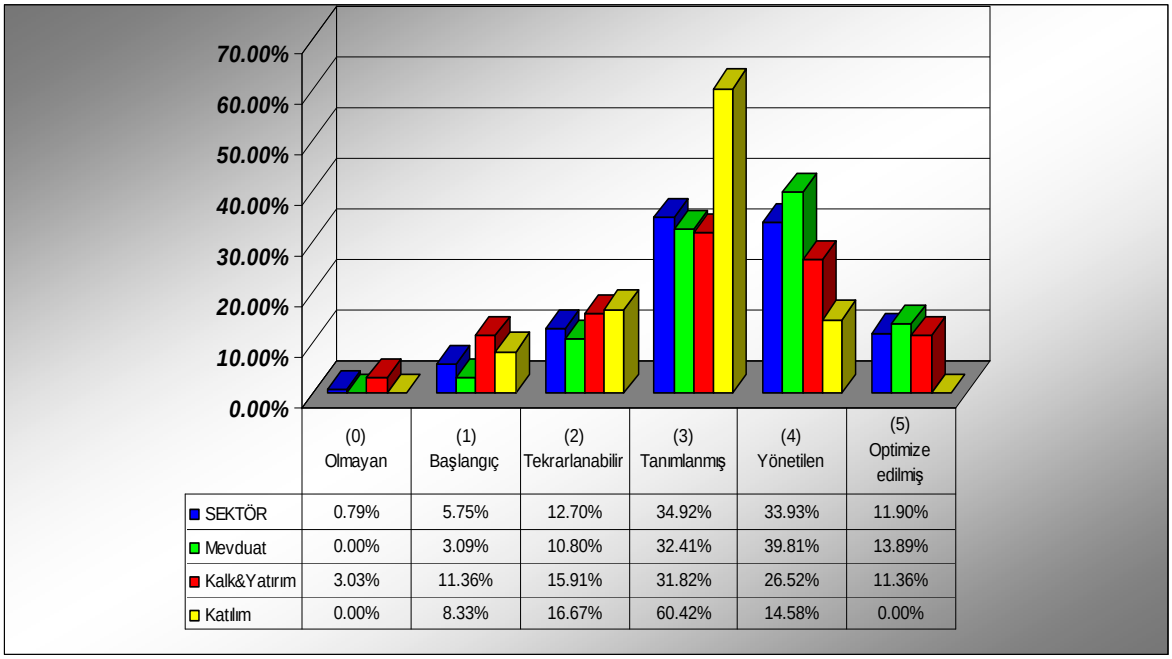
Grafik 15: Faaliyet Açısından Banka Türlerinin "Sistem" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması



	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.00%	1.79%	10.12%	33.93%	41.67%	12.50%
Mevduat	0.00%	1.39%	7.87%	29.17%	46.30%	15.28%
Kalk&Yatırım	0.00%	3.41%	13.64%	32.95%	39.77%	10.23%
Katılım	0.00%	0.00%	15.63%	68.75%	15.63%	0.00%

Süreç faktörünün analizine ilişkin veriler Grafik 16'da yer almaktadır. Bu faktör için de katılım bankalarının %60 gibi büyük oranda 3 olgunluk seviyesinde toplandıkları gözlenmektedir. Mevduat bankalarının %72'lik dağılımı 3 ila 4 olgunluk seviyelerinde olup ağırlıklı olarak 4 düzeyinde paylaşılmıştır. Kalkınma ve yatırım bankalarının bu faktör için olgunluk seviye dağılımı %32 ile 3, %27 ile 4 seviyesindedir. Sektör ortalaması da %69 ile 3 ve 4 olgunluk seviyelerinde paylaşılmıştır.

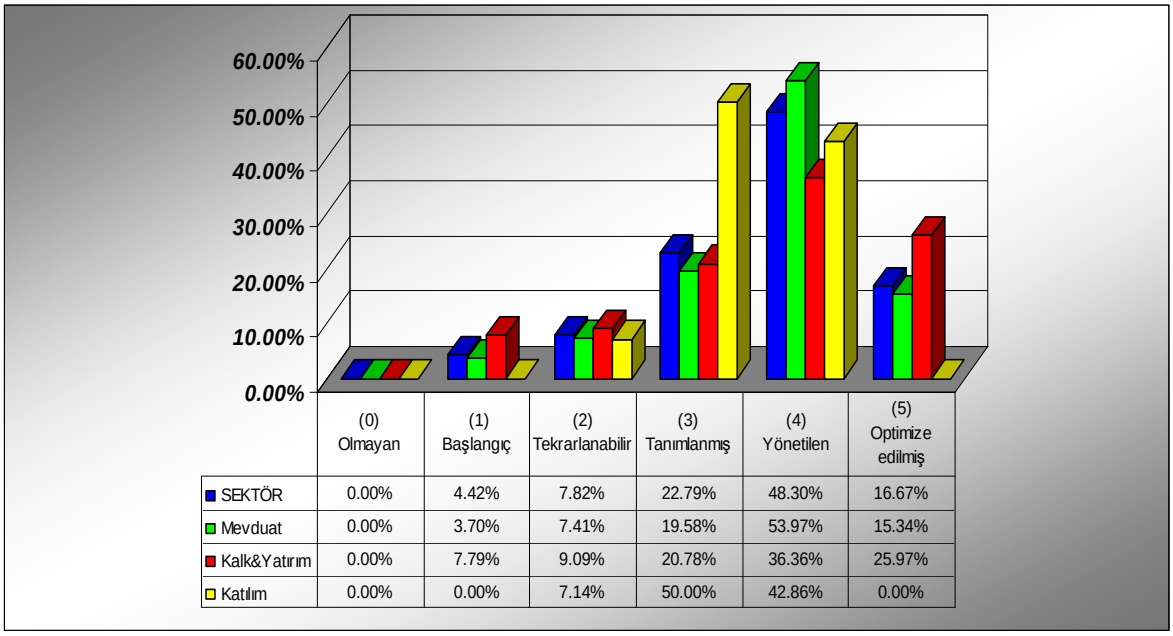
Grafik 16: Faaliyet Açısından Banka Türlerinin "Süreç" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması



	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.79%	5.75%	12.70%	34.92%	33.93%	11.90%
Mevduat	0.00%	3.09%	10.80%	32.41%	39.81%	13.89%
Kalk&Yatırım	3.03%	11.36%	15.91%	31.82%	26.52%	11.36%
Katılım	0.00%	8.33%	16.67%	60.42%	14.58%	0.00%

Dışsal etkenlere yönelik olarak banka grupları için olgunluk seviyelerinin dağılımı Grafik 17'de yer almaktadır. Mevduat bankaları %54'lük pay ile bu faktöre ilişkin ağırlıklı olarak 4(tanımlanmış) olgunluk seviyesinde bulunmaktadır. Kalkınma ve yatırım bankalarının olgunluk seviye dağılımı %21 ile 3, %36 ile 4 ve %26 ile 5 düzeyindedir. Katılım bankaları %50 ile yine ağırlıklı olarak 3 seviyesi ile %43 ile 4 seviyesinde toplanmıştır. Sektör ortalaması da %48'lik pay ile 4(yönetilen) seviyesindedir.

Grafik 17: Faaliyet Açısından Banka Türlerinin "Dışsal Etkenler" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması

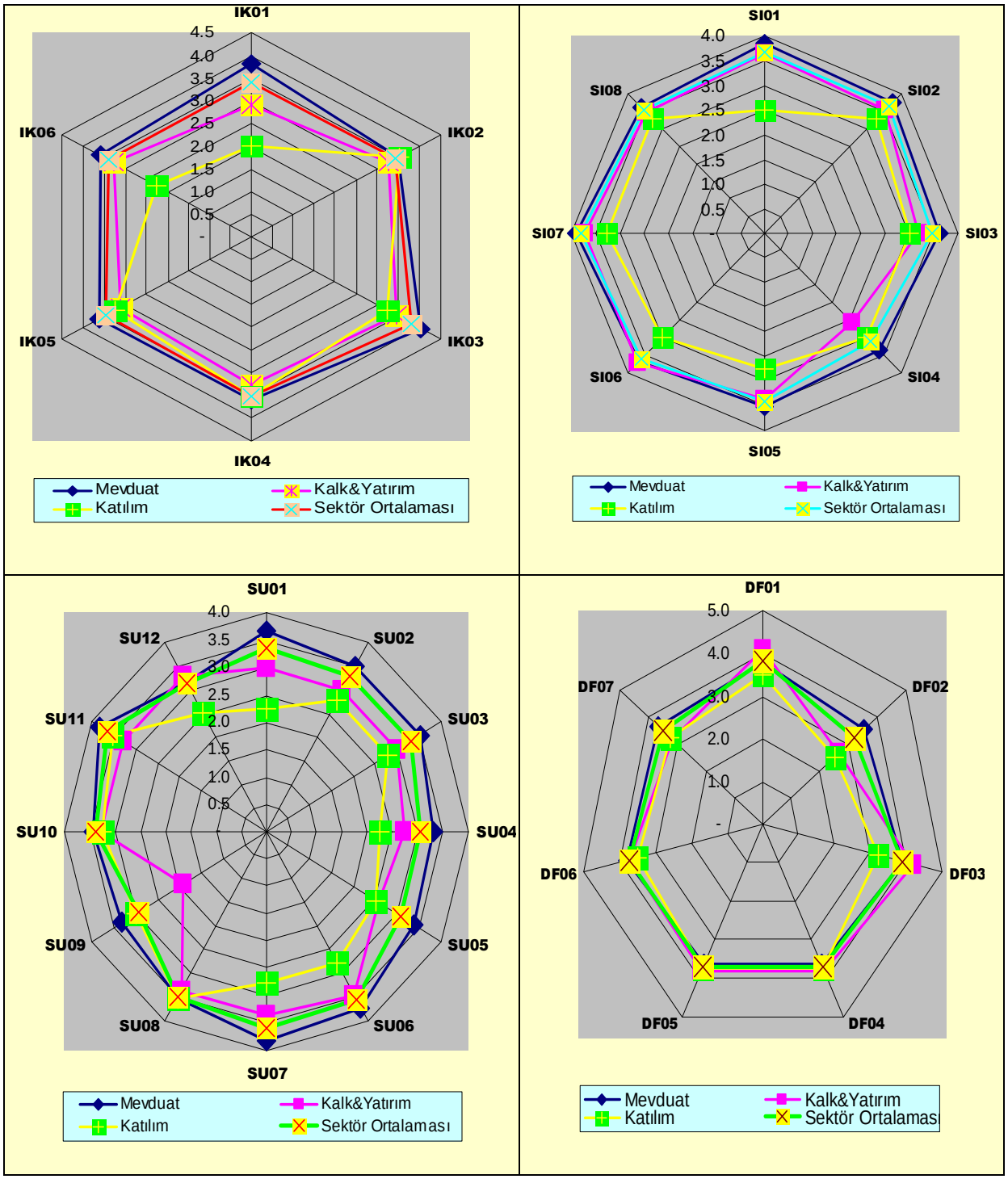


	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.00%	4.42%	7.82%	22.79%	48.30%	16.67%
Mevduat	0.00%	3.70%	7.41%	19.58%	53.97%	15.34%
Kalk&Yatırım	0.00%	7.79%	9.09%	20.78%	36.36%	25.97%
Katılım	0.00%	0.00%	7.14%	50.00%	42.86%	0.00%

Grafik 18'de faaliyet açısından banka türlerinin anketin dört ana faktörü altında yer alan alt faktörler için belirledikleri ortalama olgunluk seviyelerinin dağılımı gösterilmektedir.

Örümcek ağı şeklindeki grafiklerle banka türlerinin kendi aralarındaki olgunluk seviyeleri rahatlıkla karşılaştırılabilmektedir. Örneğin aşağıdaki grafikte yer alan şekillerde operasyonel riskin dört faktörü için de katılım bankalarının olgunluk seviye ortalamaları örümcek ağının en içinde yer alırken, mevduat bankaların ağın en dışında yani en yüksek olgunluk seviyesinde bulundukları rahat bir görsellikle sergilenmektedir.

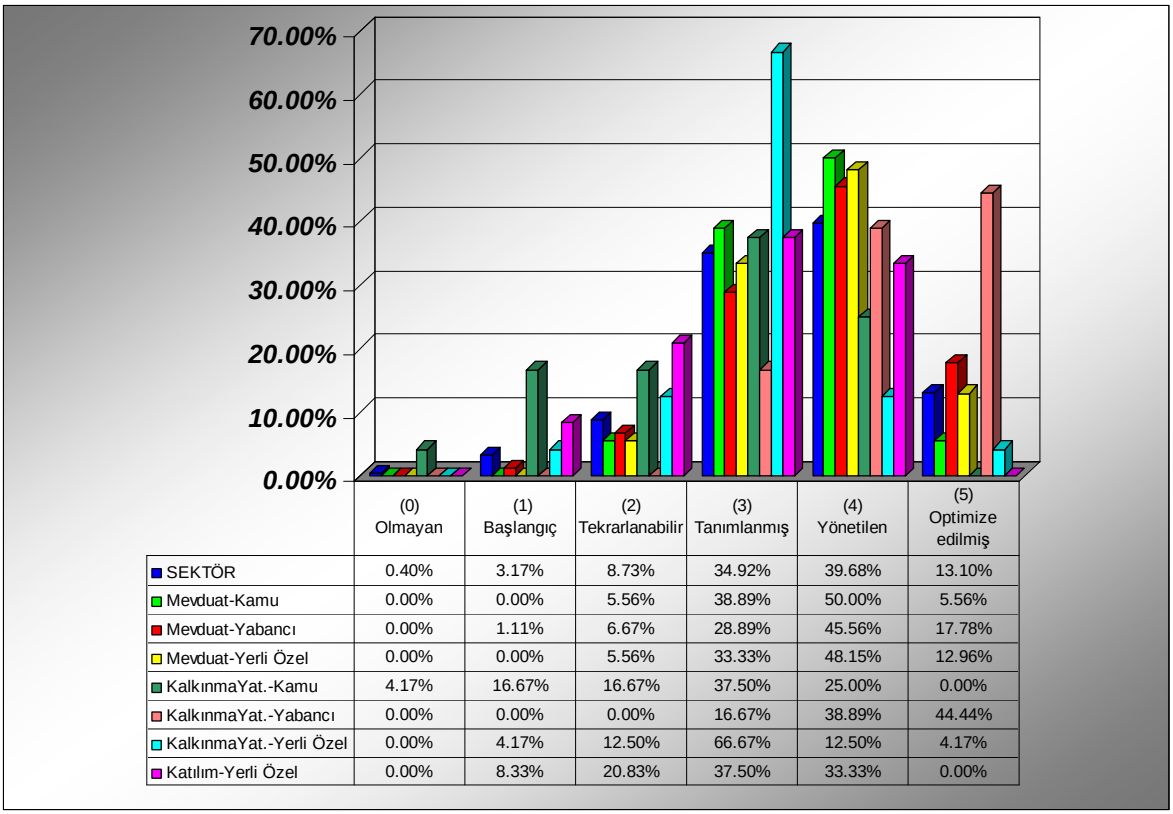
Grafik 18: Faaliyet Açısından Banka Türleri İçin Dört Ana Faktör Altındaki Alt Faktörlerin Ortalama Olgunluk Seviyeleri



4.1.9. Faaliyet ve Sahiplik Türlerine Göre Anketin Değerlendirilmesi

Bu kısımda faaliyet ve sahiplik açısından farklılık gösteren banka türlerinin dört ana faktördeki olgunluk seviyelerinin dağılımı incelenerek sektör ortalamaları ile karşılaştırılmıştır. Bankaların bu şekilde gruplamaya tabi tutulması ile "mevduat-kamu", "mevduat-yabancı", "mevduat-yerli özel", "kalkınma&yatırım-kamu", "kalkınma&yatırım yabancı", kalkınma&yatırım yerli özel" ve "katılım yerli özel" olmak üzere 7 farklı grup oluşmaktadır.

Grafik 19: Faaliyet ve Sahiplik Açısından Banka Türlerinin "İnsan" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması

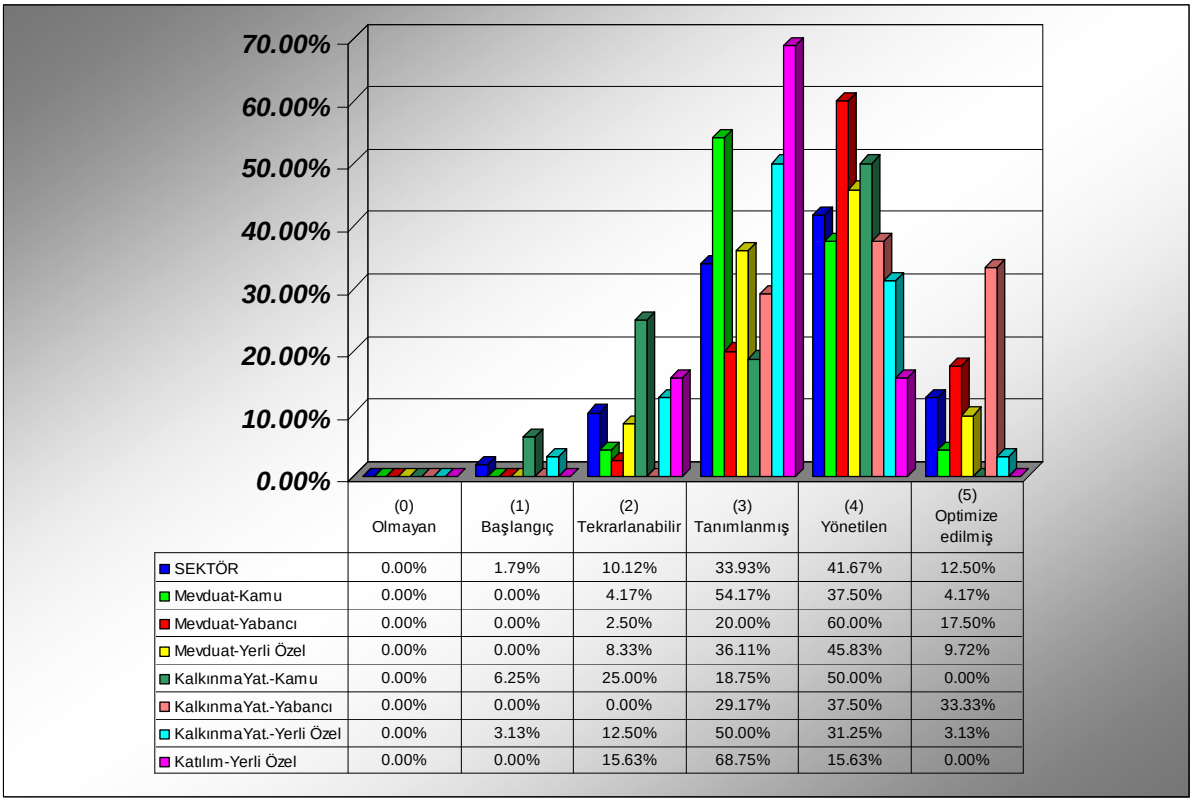


	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.40%	3.17%	8.73%	34.92%	39.68%	13.10%
Mevduat-Kamu	0.00%	0.00%	5.56%	38.89%	50.00%	5.56%
Mevduat-Yabancı	0.00%	1.11%	6.67%	28.89%	45.56%	17.78%
Mevduat-Yerli Özel	0.00%	0.00%	5.56%	33.33%	48.15%	12.96%
KalkınmaYat.-Kamu	4.17%	16.67%	16.67%	37.50%	25.00%	0.00%
KalkınmaYat.-Yabancı	0.00%	0.00%	0.00%	16.67%	38.89%	44.44%
KalkınmaYat.-Yerli Özel	0.00%	4.17%	12.50%	66.67%	12.50%	4.17%
Katılım-Yerli Özel	0.00%	8.33%	20.83%	37.50%	33.33%	0.00%

Grafik 19'da, oluşan bu 7 grubun "insan" faktörü için belirlenen olgunluk seviyelerinin yüzdesel dağılımı ve sektör ortalaması ile karşılaştırması yer almaktadır. Grafik incelendiğinde, gruplar içerisinde özellikle yabancı kalkınma ve yatırım bankalarının olgunluk seviyelerinin %44 ile 5 (optimize edilmiş), %39 ile 4 (yönetilen) derecesinde toplandıkları göze çarpmaktadır. Yani bu bankalar operasyonel riskin "insan" faktöründen

kaynaklanan yönetimini hemen hemen en iyi şekilde yapmaktadırlar. Mevduat toplayan kamu, yabancı ve yerli özel bankalara baktığımızda, bunların da %29-39 ile 3, %48-50 ile 4 olgunluk seviyesinde oldukları görülmektedir.

Grafik 20: Faaliyet ve Sahiplik Açısından Banka Türlerinin "Sistem" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması



	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.00%	1.79%	10.12%	33.93%	41.67%	12.50%
Mevduat-Kamu	0.00%	0.00%	4.17%	54.17%	37.50%	4.17%
Mevduat-Yabancı	0.00%	0.00%	2.50%	20.00%	60.00%	17.50%
Mevduat-Yerli Özel	0.00%	0.00%	8.33%	36.11%	45.83%	9.72%
KalkınmaYat.-Kamu	0.00%	6.25%	25.00%	18.75%	50.00%	0.00%
KalkınmaYat.-Yabancı	0.00%	0.00%	0.00%	29.17%	37.50%	33.33%
KalkınmaYat.-Yerli Özel	0.00%	3.13%	12.50%	50.00%	31.25%	3.13%
Katılım-Yerli Özel	0.00%	0.00%	15.63%	68.75%	15.63%	0.00%

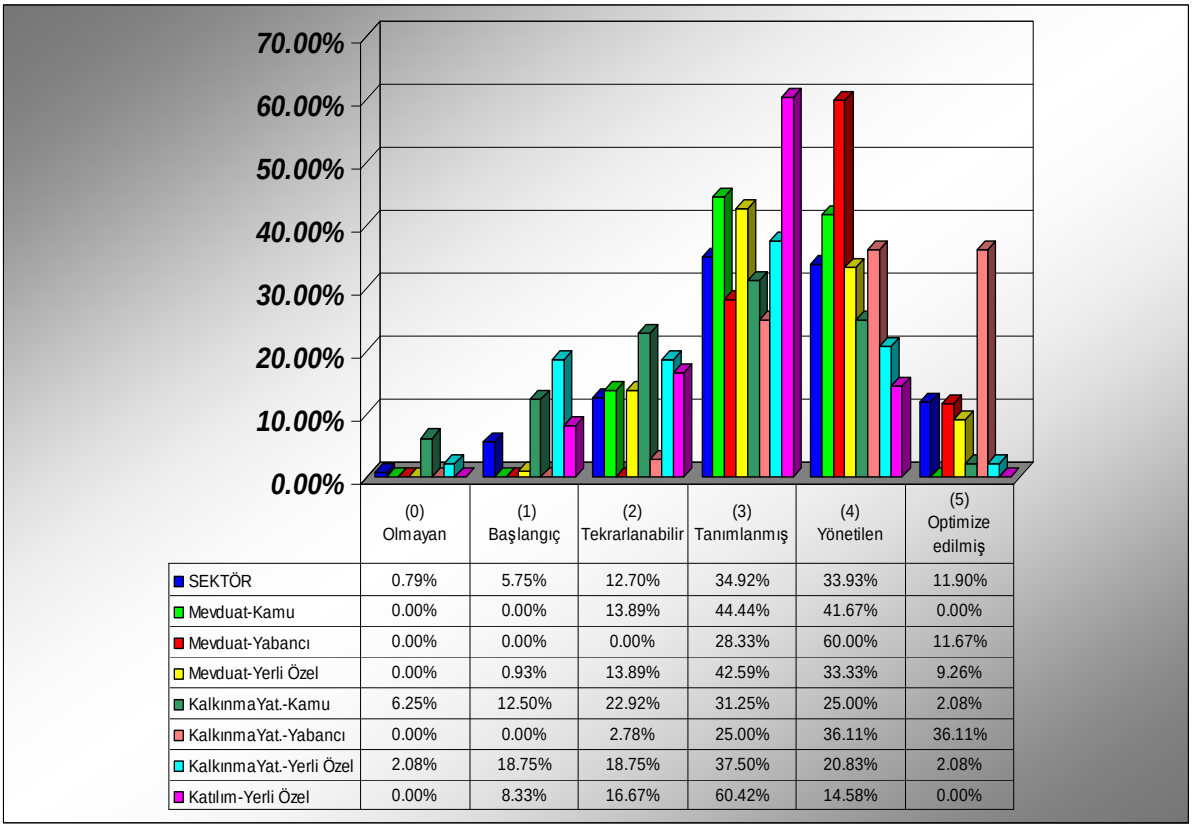
Grafik 20'de söz konusu 7 grubun "sistem" faktörü için olgunluk seviyelerinin yüzdesel dağılımı yer almaktadır. Grafik incelendiğinde ilk göze çarpan hususlar; yabancı mevduat bankalarının %60 gibi bir pay ile 4 seviyesinde oldukları, kamu mevduat bankalarının %54'lük pay ile yerli özel katılım bankalarının ise %69 gibi bir pay ile 3 seviyesinde olmasıdır. Ayrıca yabancı kalkınma ve yatırım bankalarının %33 ile 5 seviyesinde olmaları da bu konuda yüksek olgunluk seviyesinde bulunduklarını göstermektedir.

Grafik 21, sahiplik-faaliyet türlerine ayrılan bankaların "süreç" faktörüne ilişkin olgunluk seviyelerinin yüzdesel dağılımını göstermektedir. Grafikte yabancı mevduat

bankalarının olgunluk seviyesi %60 ile 4 seviyesinde bulunurken, kamu mevduat bankalarında bu dağılımın %85'lik pay ile 3 -4 civarında olduğu, katılım bankalarında %60 ile 3 seviyesinde olduğu görülmektedir.

Süreç faktörüne ilişkin sektörün ortalamasına bakıldığında ilgili banka gruplarının genelde %35 ile 3, %34 ile 4 seviyesinde oldukları görülmektedir.

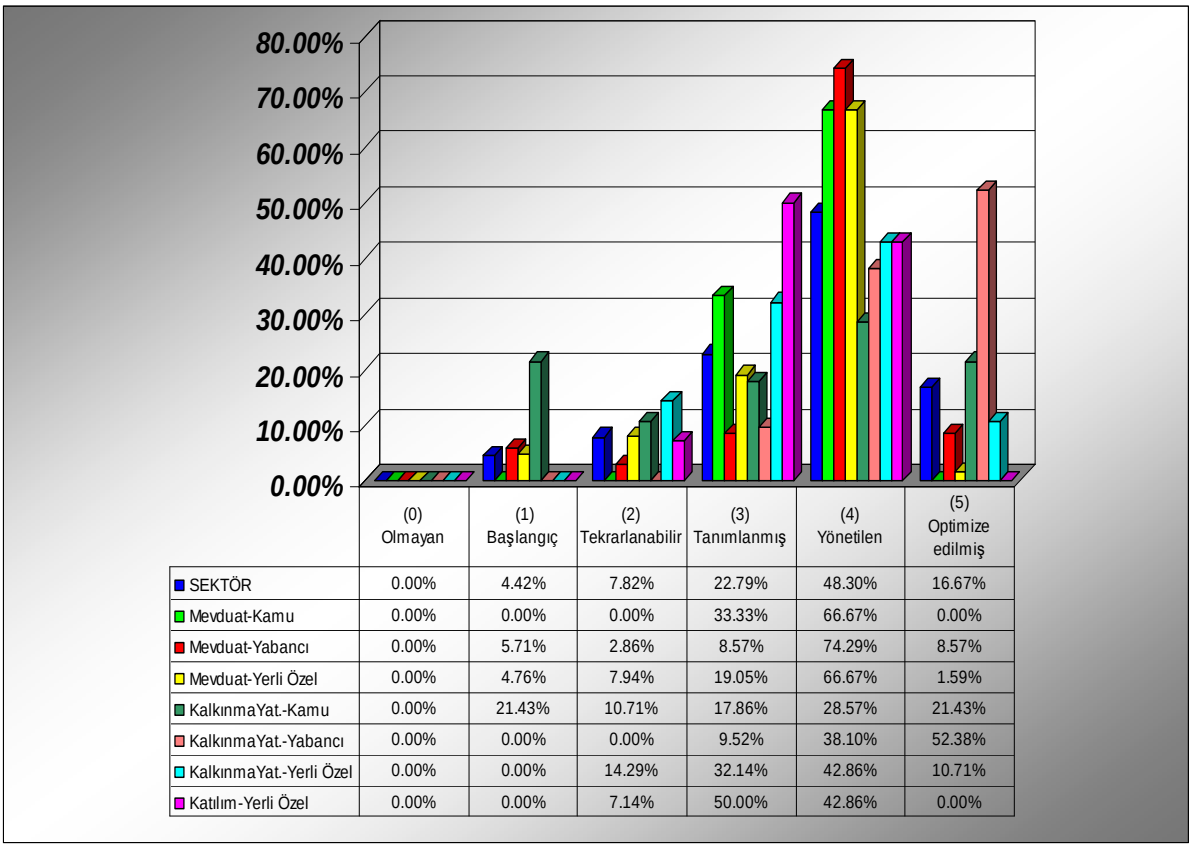
Grafik 21: Faaliyet ve Sahiplik Açısından Banka Türlerinin "Süreç" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması



	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.79%	5.75%	12.70%	34.92%	33.93%	11.90%
Mevduat-Kamu	0.00%	0.00%	13.89%	44.44%	41.67%	0.00%
Mevduat-Yabancı	0.00%	0.00%	0.00%	28.33%	60.00%	11.67%
Mevduat-Yerli Özel	0.00%	0.93%	13.89%	42.59%	33.33%	9.26%
KalkınmaYat.-Kamu	6.25%	12.50%	22.92%	31.25%	25.00%	2.08%
KalkınmaYat.-Yabancı	0.00%	0.00%	2.78%	25.00%	36.11%	36.11%
KalkınmaYat.-Yerli Özel	2.08%	18.75%	18.75%	37.50%	20.83%	2.08%
Katılım-Yerli Özel	0.00%	8.33%	16.67%	60.42%	14.58%	0.00%

Grafik 22 ilgili banka gruplarının "dışsal etkenler" faktörü için olgunluk seviyelerinin dağılımı gösterilmektedir. Buna göre kamu ve yerli özel mevduat bankalarında olgunluk seviyesinde yoğunlaşma %67'lik pay ile 4(yönetilen) seviyesinde, yabancı mevduat bankalarında %75 ile aynı seviyede görülmektedir. Yerli özel kalkınma&yatırım bankaları ile katılım bankalarında %43'lük pay ile 4 seviyesinde bir dağılım, %32-50'lik paylarla da 3 seviyesinde bir toplanma göze çarpmaktadır.

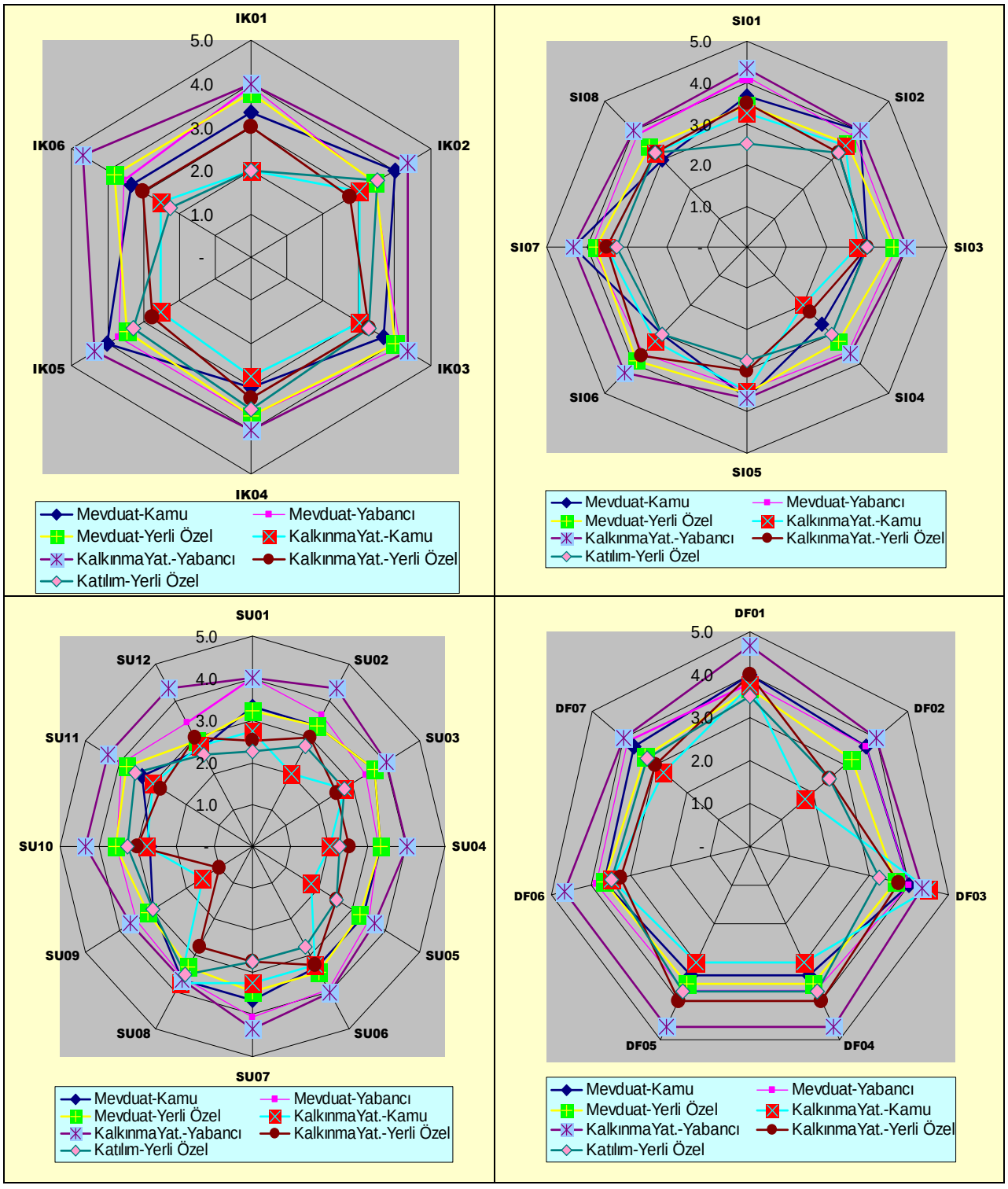
Grafik 22: Faaliyet ve Sahiplik Açısından Banka Türlerinin "Dışsal Etkenler" Faktörü İçin Olgunluk Seviyelerinin Yüzdesel Dağılımı ve Sektör Ortalaması ile Karşılaştırması



	(0) Olmayan	(1) Başlangıç	(2) Tekrarlanabilir	(3) Tanımlanmış	(4) Yönetilen	(5) Optimize edilmiş
SEKTÖR	0.00%	4.42%	7.82%	22.79%	48.30%	16.67%
Mevduat-Kamu	0.00%	0.00%	0.00%	33.33%	66.67%	0.00%
Mevduat-Yabancı	0.00%	5.71%	2.86%	8.57%	74.29%	8.57%
Mevduat-Yerli Özel	0.00%	4.76%	7.94%	19.05%	66.67%	1.59%
KalkınmaYat.-Kamu	0.00%	21.43%	10.71%	17.86%	28.57%	21.43%
KalkınmaYat.-Yabancı	0.00%	0.00%	0.00%	9.52%	38.10%	52.38%
KalkınmaYat.-Yerli Özel	0.00%	0.00%	14.29%	32.14%	42.86%	10.71%
Katılım-Yerli Özel	0.00%	0.00%	7.14%	50.00%	42.86%	0.00%

Sektör ortalamasına bakıldığında bankaların genelde dışsal faktörlerden kaynaklanan riskleri daha fazla ciddiye aldıkları ve bu konuda daha fazla önlem aldıkları, bu risklerini daha iyi yönettikleri sonucu ortaya çıkmaktadır. Sektörün olgunluk seviye ortalaması %48'lik pay ile 4 seviyesinde toplanmıştır.

Grafik 23: Faaliyet ve Sahiplik Açısından Banka Türleri İçin Dört Ana Faktör Altındaki Alt Faktörlerin Ortalama Olgunluk Seviyeleri



Grafik 23'de yer alan şekillerde sahiplik ve faaliyet türü açısından gruplara ayrılan bankaların dört ana faktör altında yer alan alt faktörlere ilişkin olgunluk seviyeleri gösterilmektedir.

Grafiğin sol üst köşesindeki şekil, "insan" faktörü altındaki alt faktörler için olgunluk seviyelerini göstermektedir. Grafik incelendiğinde ağın en iç kısmında kamu kaynaklı kalkınma&yatırım bankaları ile yerli özel katılım bankaları yer almaktadır. Aynı şeklin en dışında yabancı kalkınma&yatırım bankaları göze çarpmaktadır ki bu da bu gruptaki bankaların "insan" kaynaklı operasyonel risklerini en yüksek olgunluk seviyesinde yönettiklerini göstermektedir.

Grafiğin sağ üst köşesindeki şekil "sistem" faktörü altındaki alt faktörler için olgunluk seviyelerini göstermektedir. Burada da yabancı mevduat bankaları ile yabancı kalkınma&yatırım bankalarının olgunluk seviyelerinin diğer gruplara göre çok daha iyi olduğunu göstermektedir.

Grafiğin sol alt köşesindeki şekil "süreç" faktörü altındaki alt faktörler için olgunluk seviyelerini göstermektedir. Yabancı mevduat ve kalkınma&yatırım bankaları bu faktörde de en iyi olgunluk seviyesinde görülmektedir.

Grafiğin sağ alt köşesindeki şekil "dışsal etkenler" faktörü altındaki alt faktörler için olgunluk seviyelerini göstermektedir. Bu faktör için de kamuya ait kalkınma ve yatırım bankaları ağın e iç kısmında yer alırken yabancı sermayeli kalkınma ve yatırım bankaları ağın en dışında yer almaktadır.

4.2. İstatistiksel Analiz

Uygulamanın bu kısmında bankalara gönderilen ankete verilen cevaplarla Türkiye'de faaliyet gösteren bankaların operasyonel risk yönetimi olgunluk seviyeleri ve bu seviyelere etki eden faktörler SPSS.13'de incelenerek istatistiksel analizler yapılmıştır. SPSS analizinde kullanılan değişkenlerin tanımları ve açıklamaları Tablo 32'de yapılmıştır.

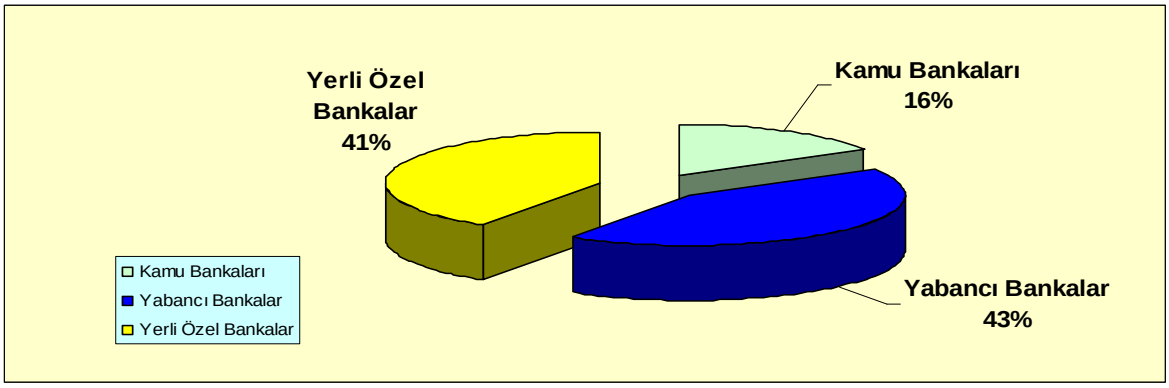
Tablo 32: SPSS Analizinde Kullanılan Değişken Tanımları ve Açıklamaları

Değişken Tanımı	Değişken Açıklaması
toppersonal	Bankalardaki toplam personel sayıları
subesayısı	Bankaların şube sayıları
ünipersonel	Bankalardaki üniversiteli personel sayısı
topaktif	Bankalardaki toplam aktif büyüklükleri
yabancısermaye	Bankaların sermayelerinin yabancı payları
egitimdüzeyi	Bankalardaki üniversitesi mezunu personelin toplam personel içindeki oranı
bankayası	Bankaların kuruluşundan bugüne dek (2009 yılı) faaliyette bulunduğu süre
genel	Operasyonel risk yönetimi performansı
insan	Operasyonel risk yönetimi performansını etkileyen insan kaynakları faktörü
sistem	Operasyonel risk yönetimi performansını etkileyen sistem faktörü
süreç	Operasyonel risk yönetimi performansını etkileyen süreç faktörü
d.faktorler	Operasyonel risk yönetimi performansını etkileyen dışsal faktörler

4.2.1. Verilerin Dağılımları ve Tanımlayıcı İstatistikleri

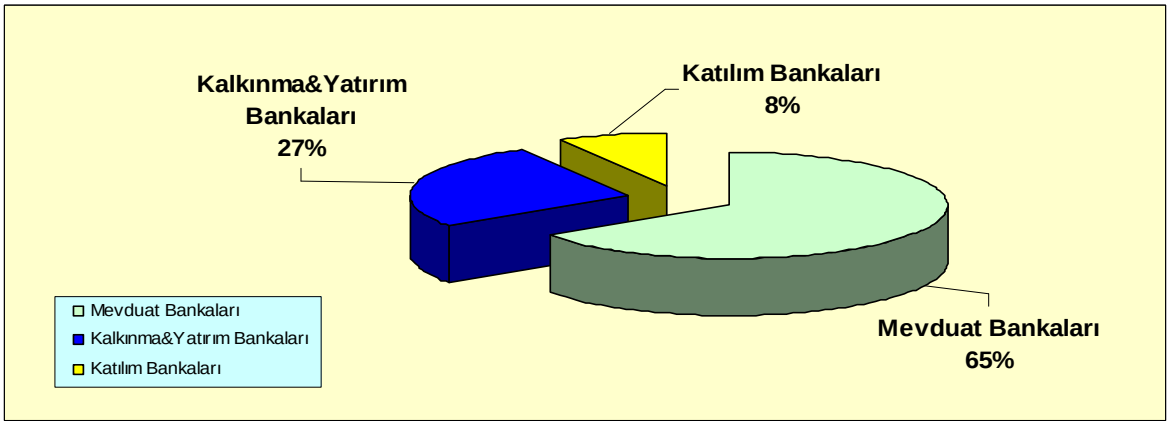
Analizde kullanılacak verilerin dağılımlarını ve yapılarını incelemek için öncelikle tanımlayıcı istatistikler ve grafikler oluşturulmuştur. Grafik 24, Türkiye'de faaliyet gösteren bankaların sahiplik açısından gruplarını ve her grubun toplam içerisindeki payını göstermektedir. Grafiğe göre bankaların %16'sını kamu bankası, %43'ü yabancı banka ve %41'i yerli özel bankadır.

Grafik 24: Sahiplik Açısından Banka Türlerinin Yüzdesel Dağılımı



Türkiye'de faaliyet gösteren bankaların faaliyet türü açısından yüzdesel dağılımı Grafik 25'de gösterilmektedir. Grafiğe göre, bu türde bankaların %65'i mevduat bankası, %27'si kalkınma ve yatırım bankası ve %8'i katılım bankası olma özelliğine sahiptir.

Grafik 25: Faaliyet Açısından Banka Türlerinin Yüzdesel Dağılımı



Tablo 33: Tanımlayıcı İstatistikler

	N	Minimum	Maximum	Mean	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
ünipersonel	49	10.00	15889.00	2793.8163	2E+007	1.803	.340	2.321	.668
toppersonal	49	16.00	21453.00	3716.7755	3E+007	1.826	.340	2.546	.668
yabancisermaye	49	.00	100.00	53.3510	1818.398	-.125	.340	-1.764	.668
subesayisi	49	1.00	875.00	143.6327	55888.446	1.858	.340	2.642	.668
topaktif	49	28.00	92338.12	13854.14	6E+008	2.221	.340	3.801	.668
egitimduzeyi	49	43.00	97.00	76.6531	128.440	-.758	.340	1.199	.668
bankayasi	49	4.00	146.00	34.5102	767.297	1.853	.340	4.263	.668
genel	49	.00	4.90	3.0131	1.981	-1.254	.340	.609	.668
insan	49	.00	4.99	3.0622	2.078	-1.252	.340	.514	.668
sistem	49	.00	5.02	3.0778	2.060	-1.246	.340	.635	.668
süreç	49	.00	4.77	2.8653	1.911	-1.061	.340	.260	.668
d.faktorler	49	.00	4.89	3.0414	2.184	-1.112	.340	.152	.668
Valid N (listwise)	49								

Her bir değişkene ilişkin betimleyici istatistikler Tablo 33'de gösterilmektedir. Bu değerler verilerin yapısını tanımlayıcı amaçla oluşturulmuş olup tek başına bir anlam ifade etmemektedirler. Tanımlayıcı istatistiklerle her bir değişkenin aldığı minimum, maksimum, ortalama değerler, varyanslar gibi değişkene ait istatistiki değerler hesaplanmıştır.

Dağılımın normal olup olmadığı araştırmacı için çok büyük önem taşımaktadır. Parametrik olmayan tekniklere kıyasla daha güçlü olan parametrik testler ancak normal olarak dağılmış veriler üzerinde uygulanabilmektedir. Burada bahsedilen güç istatistiksel güç olup reddedilmesi gereken sıfır hipotezinin gerçekten reddedilmiş olma olasılığını göstermektedir[265].

Değişkenlerin sahip oldukları dağılımların çarpıklık (skewness) ve basıklık (kurtosis) değerleri dağılımın normal olup olmadığının değerlendirilmesinde kullanılmaktadır.

Çarpıklık, dağılımın daha çok sağa mı yoksa sola mı çarpık olduğunu gösterir. Yani, verilerin daha çok ortalamanın sağına mı yoksa soluna mı kümelendiğini yansıtır. Gözlemler ortalamanın sağına ve soluna dengeli bir şekilde dağılıyorsa dağılım normal bir dağılım olup aritmetik ortalaması, modu ve medyanı birbirine eşit demektir. Çarpıklık 0'a yaklaştıkça, gözlemlerin ortalama etrafındaki dağılımı da simetrik hale gelir. Pozitif çarpıklık dağılımın daha çok sol tarafta yığıldığını ve kuyruğunun sağa çarpık olduğunu

[265] A. Ercan Gegez, **Pazarlama Araştırmaları,** 1.Baskı, İstanbul: Beta Yayınevi, 2005, s.216.

gösterir. Tersine çarpıklık negatif ise, gözlemlerin sağa tarafta yığıldığını ve kuyruğunun da sola çarpık olduğunu gösterir[266].

Basıklık(kurtosis), dağılımın nispi sivriliğini ya da yayvanlığını gösterir. Normal bir dağılım gösteren değişkenin basıklığı sıfırdır. Basıklık pozitif bir değer ise, dağılım sivri bir görünüm oluşturur. Buna karşılık, basıklık negatif bir değer çıkarsa dağılım yayvan bir şekil gösterecektir.

Dağılımın çarpıklık (skewness) ölçüsü Skp, 0'a göre değerlendirilir.

$$Sk_p = \frac{\bar{x} - \text{mod}}{s} \quad \text{veya} \quad Sk_p = \frac{3(\bar{X} - med)}{s}$$

$Sk_P < 0 \rightarrow$ Negatif çarpık(Sola)

$Sk_P > 0 \rightarrow$ Pozitif Çarpık(Sağa)

$Sk_P = 0$ ise dağılış simetrik

(20)

Dağılımın basıklık (kurtosis) ölçüsü K, 3'e göre değerlendirilir. Ancak SPSS'te değerlendirme (K-3)'e göre yapılmaktadır.

- K = 3 ise Seri "**Normal**"
- K< 3 ise Seri "**Basık**"
- K > 3 ise Seri "**Sivri**" ya da "**Yüksek**"

Tanımlayıcı istatistiklerdeki skewness değerlerine göre bankalardaki üniversite mezunu personel sayısı, toplam personel sayısı, şube sayısı, bankaların sahip olduğu toplam aktifler ve banka yaşı değişkenlerine ait çarpıklık ölçüleri 0'dan büyük olduğu için serilerin sağa çarpık olduğunu göstermektedir.

Yabancı sermaye payları, eğitim düzeyi ve operasyonel risk yönetim performansı ve performans değerlendirme kriterleri(insan kaynakları, sistem, süreç ve dışsal faktörler)

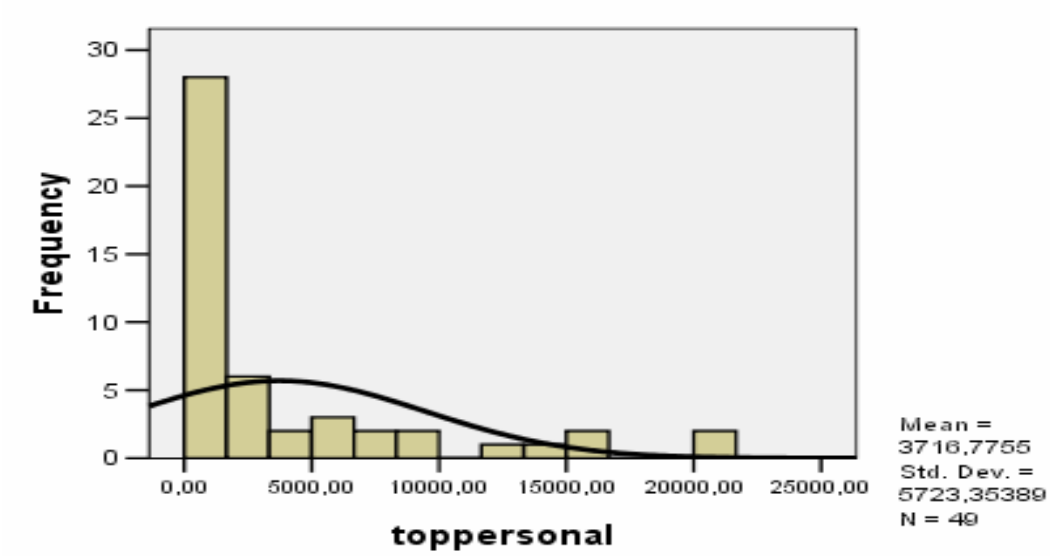
[266] Mahir Nakıp, **Pazarlama Araştırmaları ,Teknikler ve Uygulamalar,** 2.Baskı, Ankara: Seçkin Yayınevi, 2006, s.260.

değişkenlerine ait çarpıklık ölçüleri 0'dan küçük olduğu için serilerin sola çarpık olduğunu göstermektedir.

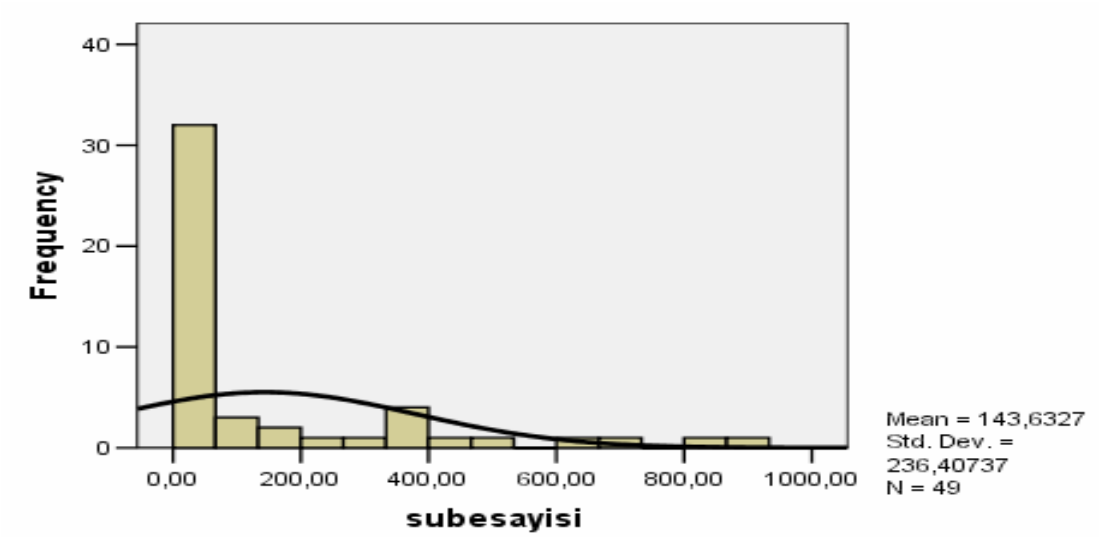
Tanımlayıcı istatistiklerdeki kurtosis değerlerine göre yabancı sermaye payı değişkenine ait kurtosis değeri 0'dan küçük olduğu için seri basıktır. Diğer tüm değişkenlere ait kurtosis değerleri 0'dan büyük olduğu için seriler sivridir.

Histogram dağılımları değişkenlere ait serilerin normal dağılıp dağılmadığı konusunda fikir veren grafiklerdir. Değişkenlere ait histogram dağılımları aşağıdaki grafiklerde gösterilmiştir.

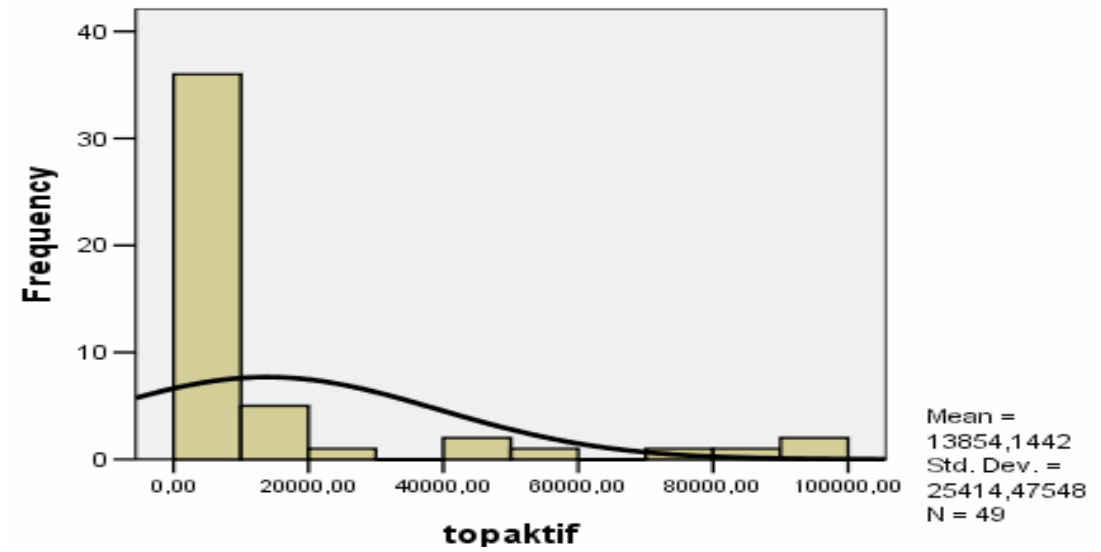
Grafik 26: Bankalardaki Personel Sayısının Histogram Dağılımı



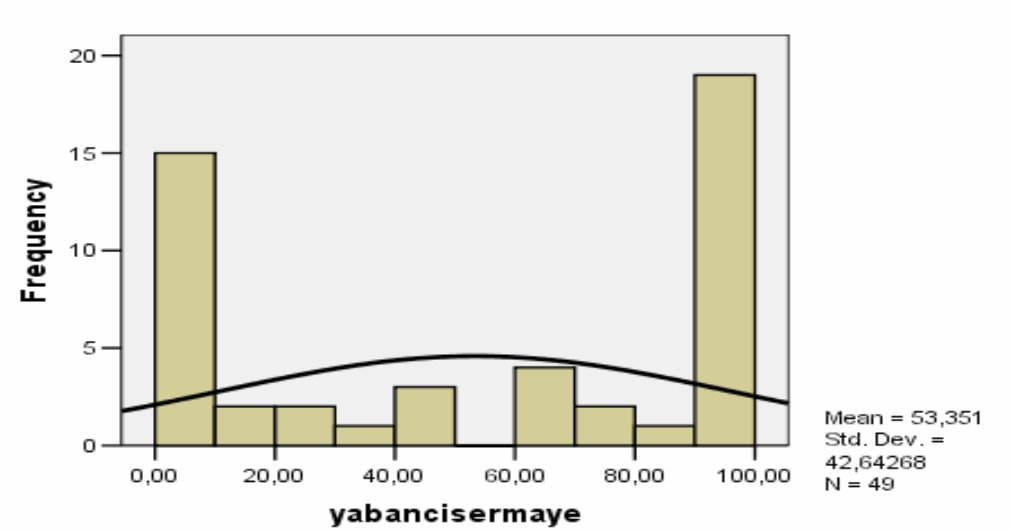
Grafik 27: Bankalardaki Şube Sayısının Histogram Dağılımı



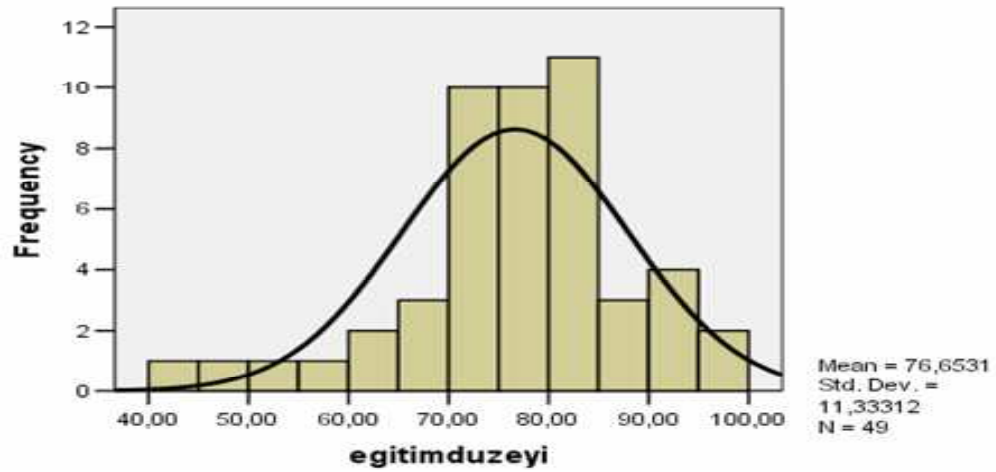
Grafik 28: Bankaların Aktif Toplamlarının Histogram Dağılımı



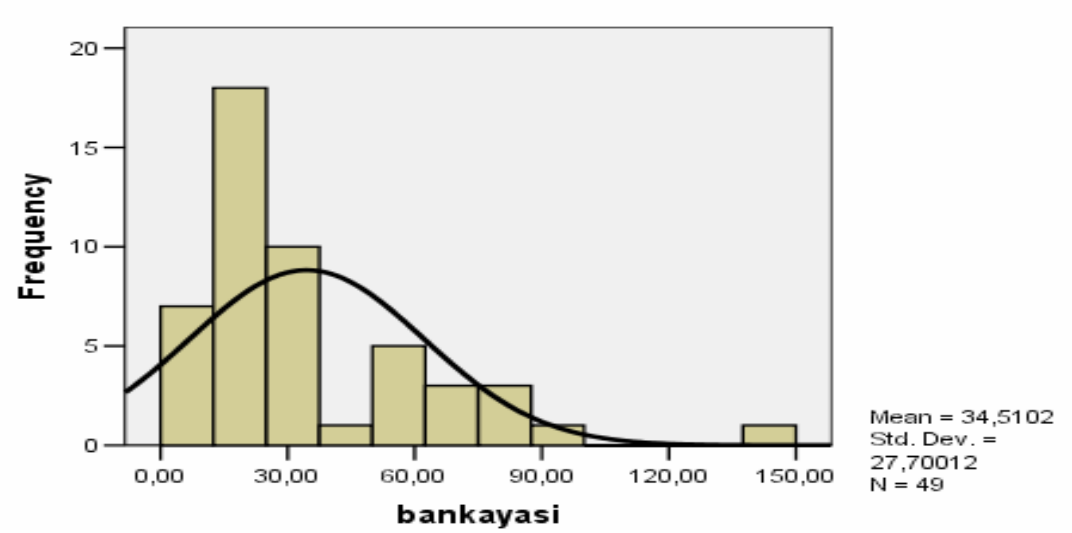
Grafik 29: Bankaların Sermayelerindeki Yabancı Payların Histogram Dağılımı



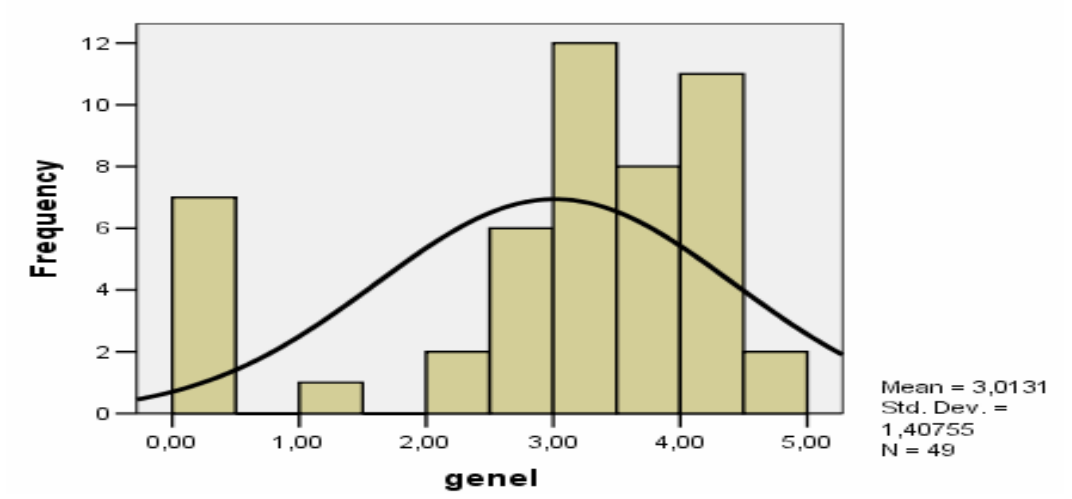
Grafik 30: Bankalardaki Üniversitesi Mezunu Personelin Toplam Personel İçindeki Oranının Histogram Dağılımı



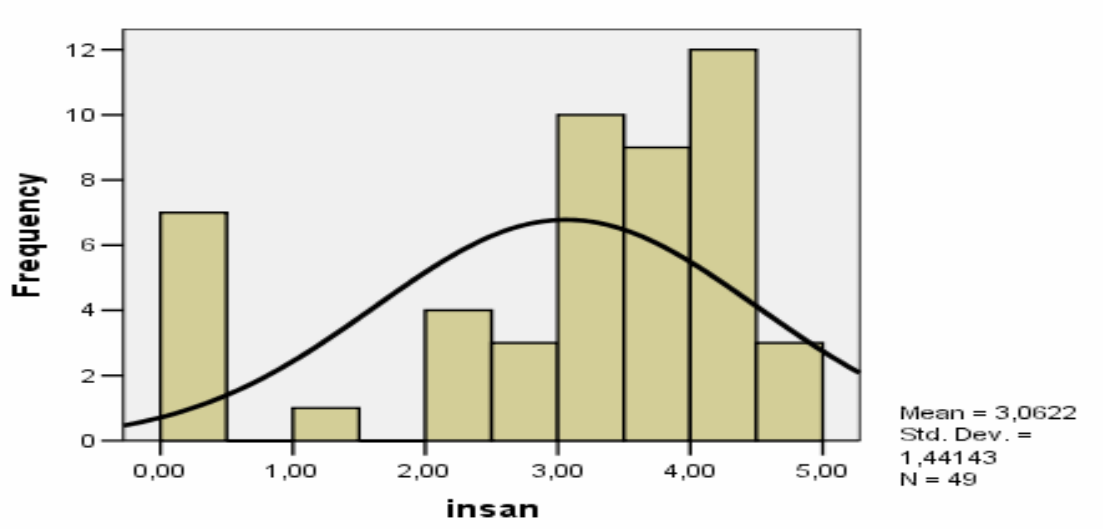
Grafik 31: Bankaların Kuruluşundan Bugüne Kadar(2009 yılı) Faaliyette Bulunduğu Süreye İlişkin Histogram Dağılımı



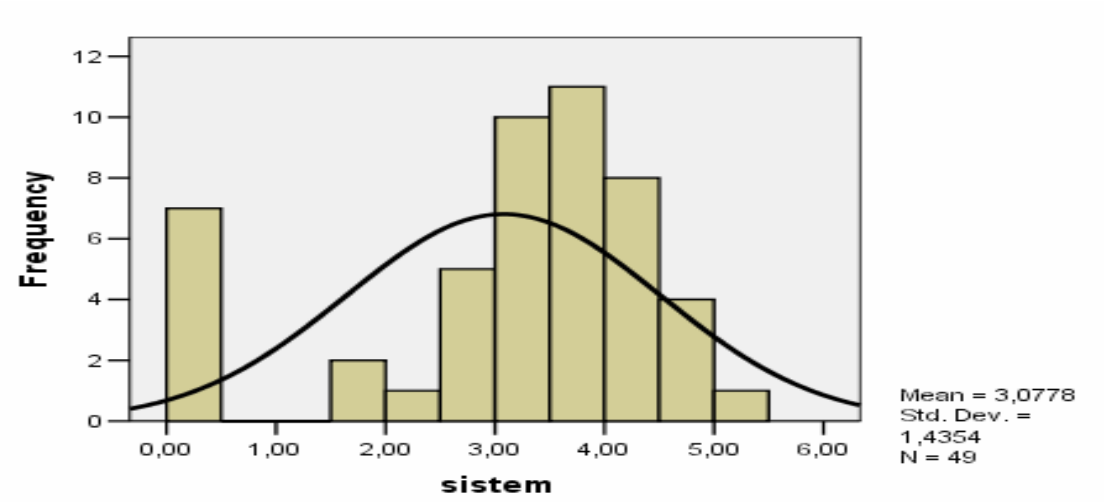
Grafik 32: Bankaların Operasyonel Risk Yönetimi Olgunluk Seviyesinin Histogram Dağılımı



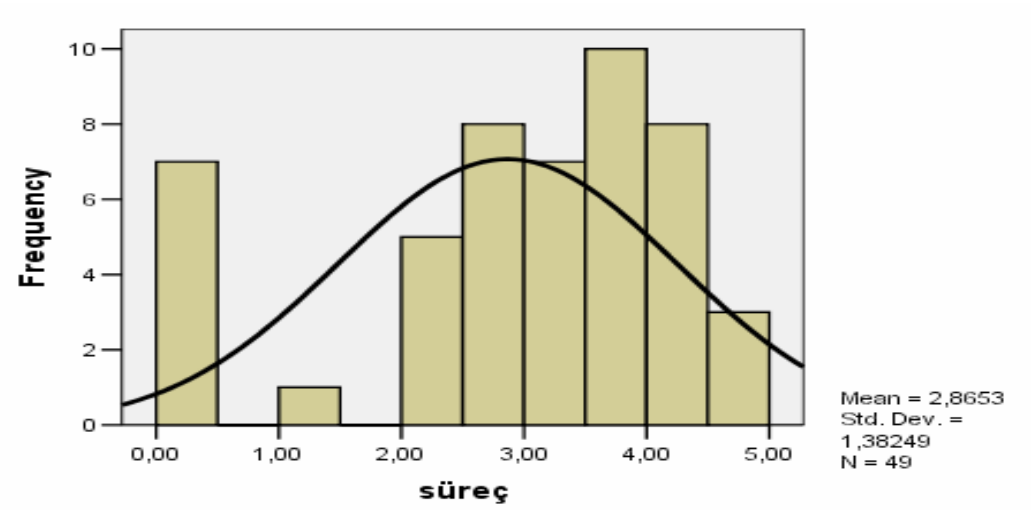
Grafik 33: Bankaların Operasyonel Risk Yönetimi Olgunluk Seviyesini Belirleyen "İnsan" Ana Faktörünün Histogram Dağılımı



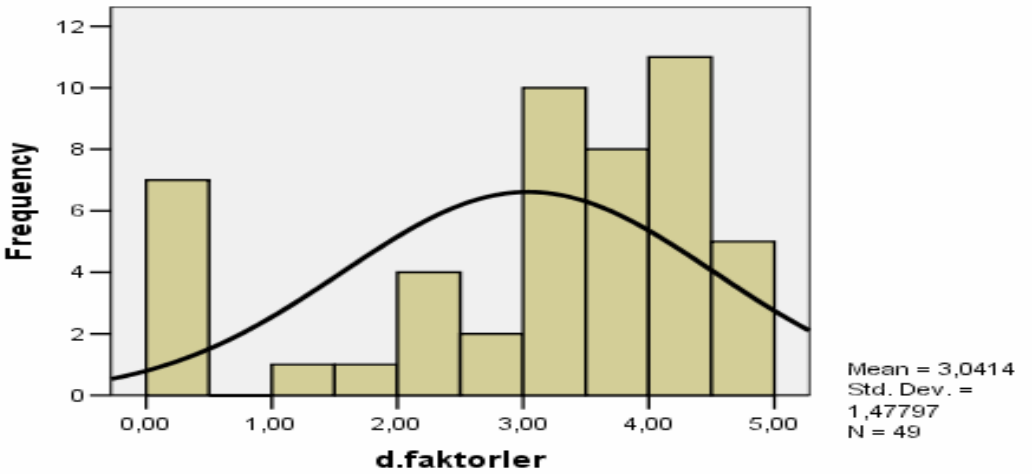
Grafik 34: Bankaların Operasyonel Risk Yönetimi Olgunluk Seviyesini Belirleyen "Sistem" Ana Faktörünün Histogram Dağılımı



Grafik 35: Bankaların Operasyonel Risk Yönetimi Olgunluk Seviyesini Belirleyen "Süreç" Ana Faktörünün Histogram Dağılımı



Grafik 36: Bankaların Operasyonel Risk Yönetimi Olgunluk Seviyesini Belirleyen "Dışsal Etkenler" Ana Faktörünün Histogram Dağılımı



4.2.2. Güvenilirlik Analizi

Güvenilirlik, aynı şeyin bağımsız ölçümleri arasındaki tutarlılıktır. Örneğin, bir tartı cihazında on kere tartıldığınızı varsayalım. Elde edeceğiniz sonuçlar birbirine ne kadar yakınsa, tartının o derece güvenilir olduğu söylenebilir. Güvenilirliği düşük olan bir ölçmenin hiçbir bilimsel değeri yoktur[267].

Sistematik hataların güvenilirlik üzerinde herhangi bir etkisi yoktur; çünkü sistematik hata sabit ve aynı şekilde ölçmeyi etkiler ve tutarsızlığa sebep olmaz. Ancak, tesadüfi hata bazı tutarsızlıklara sebep olur ve güvenirliliği zedeler. Bu nedenle güvenirliliği, tesadüfi hatalardan arınmış ölçeklerde bulmak mümkündür. Bir ölçeğin geçerli olması için, güvenilir olması gerekir; ancak güvenilir olması, geçerli olduğu anlamına gelmez[268]. Güvenirliği değerlendirebilmek için yaygın olarak kullanılan bir yaklaşım "Alfa Yöntemi(Cronbach Alfa Katsayısı)"dir.

Alfa Yöntemi(Cronbach Alfa Katsayısı): Likert ölçekli sorularda sıkça kullanılan bir yaklaşımdır. Bilindiği üzere, likert ölçeğinde genelde bir konuyu ölçen k sayıda ifade bulunmaktadır. Alfa katsayısı 0-1 arasında pozitif bir değerdir ve ağırlıklı standart değişimi gösterir. Başka bir ifadeyle, k sayıdaki ifadelerin bir bütün oluşturup oluşturmadığını, aralarındaki homojenlik derecesini gösterir. İfadeler arasındaki korelasyon ne kadar yüksek çıkarsa, alfa katsayısının da yüksek çıkma ihtimali o kadar artar. Doğru bir güvenilirlik katsayısı elde edebilmek için, gözlem sayısının ifadelerin 3 ya da 4 katı olmasında yarar vardır. Alfa katsayısı negatif çıkarsa güvenirlik modeli bozulur. Alfanın negatif çıkmasının sebebi, likert ölçeğinde hazırlanan ifadelerin bir kısmının pozitif diğer bir kısmının da negatif yönde sorulmasından kaynaklanmaktadır. İfadeler arasındaki korelasyon katsayılarının %25'ten fazla olması arzulanır.

Tablo 34'de referans aralığı şeklinde cronbach alfa katsayıları ve her referans aralığının güvenilirlik derecesi verilmiştir. Tabloya göre ölçeğin güvenilir olması için

[267] Türker Baş, **Anket Nasıl Hazırlanır, Uygulanır, Değerlendirilir?**, 4.Baskı, Ankara:Seçkin Yayıncılık, Ocak 2006, s.187.
[268] Hüner Şencan, **Sosyal ve Davranışsal Ölçümlerde Güvenilirlik ve Geçerlilik**, 1.Baskı, Ankara:Seçkin Yayıncılık, Ocak 2005, s.17.

cronbach alfa katsayısının %61-80 aralığında olması, ölçeğin çok güvenilir olması için bu katsayının %81'den yukarı olması gerekmektedir.

Tablo 34: Cronbach Alfa Katsayıları ve Güvenilirlik Dereceleri

Cronbach Alfa Katsayısı	Güvenilirlik derecesi
1-20	Hiç güvenilmez
21-40	Güvenilmez
41-60	Nispeten güvenilir
61-80	Güvenilir
81-100	Çok güvenilir

Kaynak: Beril Sipahi, E.Serra Yurtkoru ve Murat Çinko, "Sosyal Bilimlerde SPSS'le Veri Analizi", 2.Baskı, İstanbul: Beta Yayınları, 2008, s.80.

4.2.2.1. Ölçeğin Dört Ana Faktörü ve Alt Faktörleri

Bankalarda operasyonel risk yönetimine ilişkin olgunluk seviyesinin belirlenmesine yönelik hazırlanan ölçek "insan", "sistem", "süreç" ve "dışsal etkenler" olmak üzere dört ana faktörden oluşmuştur. Bu dört ana faktörün her birinin altında sırasıyla 6, 8, 12, 7 olmak üzere toplam 33 alt faktör bulunmaktadır.

Bu kısımda önce her bir ana faktör için sonra da ölçeğin tümü için güvenilirlik analizi yapılacaktır. Ölçeği oluşturan ve SPSS analizinde kullanılan alt faktör kodları, ana faktörler altında gruplanmış olup Tablo 35'de gösterilmiştir.

Tablo 35: Ölçeğin Ana Faktörleri ve Alt Faktörleri

ANA FAKTÖR	ALT FAKTÖR DEĞERLENDİRME CÜMLELERİ
İnsan	ik01, ik02, ik03, ik04, ik05, ik06
Sistem	si01, si02, si03, si04, si05, si06, si07, si08
Süreç	su01, su02, su03, su04, su05, su06, su07, su08, su09, su10, su11, su12
Dışsal Etkenler	df01, df02, df03, df04, df05, df06, df07

4.2.2.2. "İnsan" Faktörünün Güvenilirlik Analizi

"İnsan" faktörünü oluşturan ifadeler Tablo 36'da yer almaktadır.

Tablo 36: "İnsan" Faktörünü Oluşturan İfadeler

KOD	İFADELER (ALT FAKTÖRLER)
ik01	İnsan Kaynakları Yönetim Metodolojisi
ik02	Eğitim Politikası
ik03	Suiistimallerin Önlenmesi ve Etik İlkelere Uyum
ik04	Görev Tanımları
ik05	Personel İşe Alım- İşten Ayrılış Süreci
ik06	Performans Yönetimi

Operasyonel risk yönetim olgunluk seviyesine etki eden "insan" ana faktörüne ilişkin likert ölçekli değerlendirme cümlelerinin güvenilirliğini ölçmek amacıyla "Alfa Yöntemi" yaklaşımı kullanılmıştır. Buna göre, alfa katsayısı Tablo 37'den de görüleceği üzere 0.969 hesaplanmış olup, ölçeğin "İnsan" ana faktörü altında yer alan değerlendirme cümleleri çok güvenilirdir.

Tablo 37: "İnsan" Faktörünün Güvenilirlik Analizi

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.969	.970	6

Tablo 38: "İnsan" Faktörüne Ait İfadeler Arası Korelasyon Matrisi

	ik01	ik02	ik03	ik04	ik05	ik06
ik01	1.000	.816	.801	.865	.829	.835
ik02	.816	1.000	.803	.844	.858	.799
ik03	.801	.803	1.000	.851	.894	.830
ik04	.865	.844	.851	1.000	.899	.867
ik05	.829	.858	.894	.899	1.000	.866
ik06	.835	.799	.830	.867	.866	1.000

The covariance matrix is calculated and used in the analysis.

Tablo 38, operasyonel risk faktörüne etki eden insan kaynakları faktörüne ilişkin hazırlanmış likert ölçeğinde yer alan ifadeler arasındaki ilişki katsayılarını göstermektedir. İfadeler arasındaki korelasyon(ilişki) katsayılarının tümü %25 seviyesinden yüksektir. Bu da söz konusu ifadeler arasında bir bütünlük olduğunu göstermektedir.

4.2.2.3. “Sistem” Faktörünün Güvenilirlik Analizi

“Sistem” faktörünü oluşturan ifadeler Tablo 39’da verilmektedir.

Tablo 39: “Sistem” Faktörünü Oluşturan İfadeler

KOD	İFADELER (ALT FAKTÖRLER)
si01	Bilgi Teknolojileri Risk Tanımlama ve Değerlendirme
si02	Bilgi Teknolojileri Alt Yapısının Yenileme ve Bakımı
si03	Uygulamaların Test Edilmesi
si04	Bilgi Teknolojileri Performans ve Kapasite Yönetimi
si05	Değişiklik Yönetimi
si06	Bilgi Teknolojileri İş Süreklilik Planı
si07	Bilgi Güvenlik Politikası
si08	Bilgi Güvenlik Test ve Analizleri

Tablo 40: “Sistem” Faktörünün Güvenilirlik Analizi

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.982	.982	8

Operasyonel risk yönetimi performans kriterlerinden olan sistem faktörüne ilişkin likert ölçekli değerlendirme cümlelerine uygulanan güvenirlilik analizi sonucunda alfa katsayısı 0.982 çıkmıştır. Bu da “sistem” faktörü altında yer alan değerlendirme cümlelerinin çok güvenilir olduğunu göstermektedir.

Tablo 41: "Sistem" Faktörüne Ait İfadeler Arası Korelasyon Matrisi

	si01	si02	si03	si04	si05	si06	si07	si08
si01	1.000	.888	.865	.879	.862	.911	.899	.893
si02	.888	1.000	.902	.846	.824	.895	.893	.858
si03	.865	.902	1.000	.848	.777	.859	.857	.835
si04	.879	.846	.848	1.000	.818	.886	.856	.854
si05	.862	.824	.777	.818	1.000	.901	.875	.840
si06	.911	.895	.859	.886	.901	1.000	.918	.916
si07	.899	.893	.857	.856	.875	.918	1.000	.911
si08	.893	.858	.835	.854	.840	.916	.911	1.000

The covariance matrix is calculated and used in the analysis.

Tablo 41'de yer alan sistem faktörüne ait ifadeler arasındaki korelasyon katsayılarının tümü %25 ten büyük olduğundan ifadeler arasında bütünlük sağlanmıştır denebilir.

4.2.2.4. "Süreç" Faktörünün Güvenilirlik Analizi

"Süreç" faktörünü oluşturan ifadeler Tablo 42'de verilmektedir.

Tablo 42: "Süreç" Faktörünü Oluşturan İfadeler

KOD	İFADELER (ALT FAKTÖRLER)
su01	Operasyonel Risk Yönetiminde Kurum Kültürü
su02	Operasyonel Risk Kayıp Veritabanı
su03	Operasyonel Riskin Tanımlanması ve Değerlendirilmesi
su04	Operasyonel Riskin Ölçülmesi
su05	Operasyonel Riske Karşı Aksiyon Alınması
su06	İç Kontrol Sistemi
su07	Kurumsal Risk Yönetimi
su08	Proje Geliştirme
su09	Kalite Yönetimi
su10	Kontrollere İlişkin Dokümantasyon
su11	Operasyonel İşlem Limitlerinin Belirlenmesi
su12	Problem Yönetimi

Tablo 43: "Süreç" Faktörünün Güvenilirlik Analizi

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.981	.982	12

Operasyonel risk yönetimi performans kriterlerinden olan "süreç" faktörüne ilişkin likert ölçekli değerlendirme cümlelerine güvenirlik analizi yapılmış ve Tablo 43'den de görüleceği üzere alfa katsayısı 0.981 bulunmuştur. Bu oran oldukça iyi bir oran olup süreç faktörüne ilişkin değerlendirme cümlelerinin çok güvenilir olduğunu göstermektedir.

Tablo 44: "Süreç" Faktörüne Ait İfadeler Arası Korelasyon Matrisi

	su01	su02	su03	su04	su05	su06	su07	su08	su09	su10	su11	su12
su01	1.000	.852	.895	.837	.877	.827	.880	.827	.829	.813	.804	.868
su02	.852	1.000	.856	.796	.825	.745	.783	.778	.834	.780	.738	.835
su03	.895	.856	1.000	.892	.884	.803	.835	.840	.834	.833	.837	.810
su04	.837	.796	.892	1.000	.922	.790	.851	.701	.778	.825	.774	.758
su05	.877	.825	.884	.922	1.000	.841	.871	.733	.832	.817	.826	.808
su06	.827	.745	.803	.790	.841	1.000	.883	.832	.734	.872	.779	.761
su07	.880	.783	.835	.851	.871	.883	1.000	.853	.844	.875	.784	.835
su08	.827	.778	.840	.701	.733	.832	.853	1.000	.779	.853	.778	.809
su09	.829	.834	.834	.778	.832	.734	.844	.779	1.000	.787	.777	.778
su10	.813	.780	.833	.825	.817	.872	.875	.853	.787	1.000	.774	.797
su11	.804	.738	.837	.774	.826	.779	.784	.778	.777	.774	1.000	.819
su12	.868	.835	.810	.758	.808	.761	.835	.809	.778	.797	.819	1.000

The covariance matrix is calculated and used in the analysis.

Tablo 44'den de görüleceği üzere süreç faktörüne ilişkin yer alan ifadeler arasında bütünlüğün sağlandığı, ifadeler arasındaki korelasyon katsayılarının oldukça yüksek olmasından anlaşılmaktadır.

4.2.2.5. “Dışsal Etkenler” Faktörünün Güvenilirlik Analizi

“Dışsal Etkenler” faktörünü oluşturan ifadeler Tablo 45’de verilmektedir.

Tablo 45: “Dışsal Etkenler” Faktörünü Oluşturan İfadeler

KOD	İFADELER (ALT FAKTÖRLER)
df01	Tedarikçi Performans Değerlendirmesi
df02	İş Sürekliliğinin Sağlanması
df03	Acil durum ve İş Süreklilik Planı Testleri
df04	Elektronik Veri ve Kritik Dokümanların Yedeklenmesi
df05	Acil Durum Merkezinin Kurulması
df06	Acil Durum ve İş Süreklilik Eğitimleri
df07	Fiziksel ve Çevresel Güvenlik

Operasyonel risk yönetimi performans kriterlerinden olan “dışsal faktörler”e ilişkin likert ölçekli değerlendirme cümleleri için yapılan güvenirlilik analizinde alfa katsayısı 0.980 olarak bulunmuştur (Bkz.Tablo 46). Bu da dışsal faktörlere ilişkin likert ölçekte hazırlanmış ifadelerin çok güvenilir olduğunu göstermektedir

Tablo 46: “Dışsal Etkenler” Faktörünün Güvenilirlik Analizi

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.980	.981	7

Dışsal faktörlere ilişkin ifadelerin arasındaki yüksek orandaki korelasyon katsayılarını gösteren Tablo 47’den de anlaşılacağı gibi dışsal faktörlere ilişkin likert ölçek düzeyinde hazırlanmış ifadeler arasında bütünlük sağlanmıştır.

Tablo 47: "Dışsal Etkenler" Faktörüne Ait İfadeler Arası Korelasyon Matrisi

	df01	df02	df03	df04	df05	df06	df07
df01	1.000	.843	.891	.880	.880	.915	.894
df02	.843	1.000	.768	.821	.821	.870	.853
df03	.891	.768	1.000	.850	.850	.933	.880
df04	.880	.821	.850	1.000	1.000	.918	.891
df05	.880	.821	.850	1.000	1.000	.918	.891
df06	.915	.870	.933	.918	.918	1.000	.913
df07	.894	.853	.880	.891	.891	.913	1.000

The covariance matrix is calculated and used in the analysis.

4.2.2.6. Ölçeğin Tümünün Güvenilirlik Analizi

Bankaların operasyonel risk yönetimi olgunluk seviyesini ölçmek için hazırlanmış ölçeğin tümü için alfa katsayısının incelenmesi sonucunda bu değerin Tablo 48'de 0.994 olduğu görülmektedir ki bu da operasyonel risk yönetimi kriterlerine ilişkin hazırlanmış likert ölçekli ifadelerin çok güvenilir olduğunu göstermektedir.

Tablo 48:Ölçeğin Tümünün Güvenilirliği

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.994	.994	33

4.2.3. Korelasyon Analizi

İki değişken arasındaki ilişkinin derecesini ve yönünü belirlemek amacıyla en sık kullanılan istatistiki yönetmelerden birisi korelasyon analizidir. Değişkenler arasındaki ilişkinin yönü ve derecesinin ölçülmesinde korelasyon katsayısından faydalanılır. Korelasyon katsayısı -1 ile +1 arasında değişen değerler alır. Korelasyon katsayısının 1'e yaklaşması ilişkinin güçlü, 0'a yaklaşması ise ilişkinin zayıf olduğunu gösterir. Korelasyon katsayısının işareti iki değişken arasındaki ilişkinin yönünü gösterir. İşaret eksi (-) ise bu iki değişken arasındaki ilişkinin ters yönlü (negatif) olduğunu, işaret (+) ise bu iki değişken arasındaki ilişkinin aynı yönlü (pozitif) olduğunu gösterir.[269]

Korelasyon katsayısının yorumunu, tam değerler dışında ara değerler için yapmak oldukça güçtür. Ara değerlerdeki korelasyon katsayısı değerlendirilirken örnek gözlem sayısı oldukça önemlidir. Çok fazla gözleme dayanan değerlendirmelerde 0.25'e kadar düşmüş bir korelasyon katsayısı bile anlamlı sayılabilmektedir. Fakat az sayıda, 10-15 gözleme dayanan değerlendirmelerde korelasyon katsayısının 0.71'in üstünde olması beklenir. Korelesyon katsayısının aldığı değerlerle deşken arasındaki ilişkinin kuvveti Tablo 49'da değerlendirilmektedir;

Tablo 49: Korelasyon Katsayısı ve İlişki Derecesi

Korelasyon Katsayısı (%)	İlişki Derecesi
0	İlişki yok
01-10	Çok zayıf
11-20	Nispeten çok zayıf
21-30	Zayıf
31-40	Nispeten zayıf
41-50	Çok az zayıf
51-60	Çok az güçlü
61-70	Nispeten güçlü
71-80	Güçlü
81-90	Nispeten çok güçlü
91-100	Çok güçlü

[269] Fazıl Güler, **İstatistik Metodları ve Uygulamaları**, İstanbul:Beta, 2005, s.254.

Doğrusal ilişkileri ortaya çıkaran bu analiz, doğrusal olmayan bir ilişkide anlamlı çıkmayabilmektedir. Korelasyon katsayısı, bir değişkendeki değişimin ne kadarını açıkladığını göstermektedir. Karşılıklı ilişkiyi gösteren korelasyon, sebep-sonuç ilişkisini göstermediği için, bir bağımlı ve bir bağımsız değişken arasında aranabildiği gibi, iki bağımlı ya da iki bağımsız değişken arasında da aranabilir.

X ve Y diye adlandırabileceğimiz n adet gözlem değerine ait, iki değişken grup varsa, (iki grup aralarında neden sonuç ilişkisi olan gruplar da olabilir) bu gruplar arasındaki korelasyona, aşağıda verilen formül dahilinde, açıklamalarda belirtilmiş işlemler yapılarak bakılmaktadır[270].

$$r = \frac{\sum_{i=1}^{n} x_i \cdot y_i}{\sqrt{\left(\sum_{i=1}^{n} x_i^2\right) \cdot \left(\sum_{i=1}^{n} y_i^2\right)}} \qquad \textbf{(21)}$$

1. X ve Y, n adet gözlemden oluşan iki değişken gözlem dizidir.
2. $(Y - \bar{Y}) = y$ olarak, $(X - \bar{X}) = x$ olarak ifade edilirler. Tüm gözlem değerleri ortalamadan çıkarılarak x ve y dizileri oluşturulur.
3. x ile y dizisinin değerleri teker teker çarpılır. Toplamları bulunur.
4. x dizisinin ve y dizisinin ayrı ayrı kareleri alınır. Toplamları bulunur.
5. x ile y dizisinin çarpılarak toplamları alınmış değer (kesrin payı), x dizisinin karesi alınarak toplamı bulunmuş değer ile y dizisinin karesi alınarak toplamı bulunmuş değerler çarpılarak karekökü bulunur (kesrin paydası).Kesrin payı paydaya bölünür.

[270] Beril Sipahi, E.Serra Yurtkoru ve Murat Çinko, **Sosyal Bilimlerde SPSS'le Veri Analizi**, 2.Baskı, İstanbul:Beta Yayınları, 2008, s.144.

4.2.3.1. ORYOS Endeksinin Eğitim Düzeyi ile Korelasyonu

Tablo 50, bankalardaki personelin eğitim düzeyi ile bankaların operasyonel risk olgunluk seviyesi arasındaki ilişkinin derecesini(korelasyon katsayısını) göstermektedir. Buna göre, personelin eğitim düzeyiyle bankaların operasyonel risk yönetimi olgunluk seviyesi arasındaki ilişki pozitiftir, yani,eğitim seviyesi arttıkça bankaların operasyonel risk yönetim başarısı da artmaktadır. Ancak, personelin eğitim seviyesiyle bankaların operasyonel risk yönetim olgunluk seviyesi arasındaki ilişkinin derecesi yaklaşık %39 olup ilişki nispeten zayıf bir ilişkidir.

Tablo 50: Eğitim Düzeyi ile Operasyonel Risk Yönetim Olgunluk Seviyesi Arasındaki Korelasyon

		egtmdüzeyi	genel
egtmdüzeyi	Pearson Correlation	1	.386(**)
	Sig. (2-tailed)		.006
	N	49	49
genel	Pearson Correlation	.386(**)	1
	Sig. (2-tailed)	.006	
	N	49	49

** Correlation is significant at the 0.01 level (2-tailed).

4.2.3.2. ORYOS Endeksinin Yabancı Sermaye Oranı ile Korelasyonu

Tablo 51, bankalardaki yabancı sermaye oranı ile bankaların operasyonel risk yönetim başarısı arasındaki ilişkinin yönü ve derecesi hakkında bilgi veren korelasyon katsayısını göstermektedir. İlişkinin yönü pozitif olup, derecesi oldukça düşüktür. Ancak, ilişkinin yönü ve derecesinden daha da önemli olan bir şey, ilişkinin istatistiksel olarak anlamlı olmamasıdır. Bunu, 0.01 hata payıyla[271] kuyruk olasılığı karşılaştırmasından anlayabiliriz.(α=0.01<kuyruk olasılığı[272]=0.08 olduğundan korelasyon katsayısı istatistiksel

[271] Ne zaman bir anakütle hakkında tahmin yapmaya çalışsak,hatalı bir sonuç çıkarma ihtimalini gözden uzak tutmamamız gerekir.Analizde %1 hata payıyla çalışılmıştır.Hata payının,tıp gibi insan sağlığı ile ilgili alanlarda %1 ve daha altında olması arzulanır.Riskin daha az olduğu diğer sosyal bilimlerde bu oran 0.1'e kadar çıkabilmektedir.Bir çok araştırma α'nın düşük düzeyde tutulmasının daha gerçekçi olacağını söylemektedir.
[272] Kuyruk olasılığı,Ho'ı reddedebileceğimiz en düşük olasılık düzeyidir.

olarak anlamsızdır.) Bu durum, bankaların yabancı sermaye payı ile operasyonel risk yönetim başarıları arasında doğrusal bir ilişkinin olmadığının göstermektedir.

Tablo 51: Yabancı Sermaye Oranı ile Operasyonel Risk Yönetim Olgunluk Seviyesi Arasındaki Korelasyon

		genel	yabancisermaye
genel	Pearson Correlation	1	.257
	Sig. (2-tailed)		.075
	N	49	49
yabancisermaye	Pearson Correlation	.257	1
	Sig. (2-tailed)	.075	
	N	49	49

Bankaların yabancı sermaye oranıyla operasyonel risk yönetim faktörleri arasında doğrusal ilişkinin olmamasından dolayı, değişkenler arasındaki eğrisel ilişkinin olup olmadığı konusunda bilgi veren Spearman korelasyon katsayısı Tablo 52'de hesaplanmıştır. Buna göre, bankaların yabancı sermaye oranıyla operasyonel risk yönetim faktörleri arasında eğrisel bir ilişki söz konusudur.

(α=0.01>kuyruk olasılığı=0.001olduğundan Spearman korelasyon katsayısı istatistiksel olarak anlamlıdır.) Bankaların yabancı sermaye oranı ile operasyonel risk yönetim performansı arasında pozitif bir ilişki vardır, yani bankalardaki yabancı sermaye oranı arttıkça bankaların operasyonel risk yönetim başarısı da artmaktadır.

Tablo 52: Yabancı Sermayeli Bankalarla Operasyonel Risk Yönetim Olgunluk Seviyeleri Arasındaki Eğrisel İlişki Korelasyonu

Spearman's rho	genel	Correlation Coefficient	1.000	.463(**)
		Sig. (2-tailed)	.	.001
		N	49	49
	yabancisermaye	Correlation Coefficient	.463(**)	1.000
		Sig. (2-tailed)	.001	.
		N	49	49

** Correlation is significant at the 0.01 level (2-tailed).

4.2.3.3. ORYOS Endeksinin Yabancılaşma Süreleri ile Korelasyonu

Tablo 53'deki korelasyon katsayısı, yabancı bankaların yabancılaşma süreleri ile bu bankaların operasyonel risk yönetimi arasındaki ilişkiyi göstermektedir. İlişkinin yönü pozitif çıkmış olup, ilişkinin derecesi 0.25'tir. Buna göre, yabancı bankalar arasında kuruluş tarihinden itibaren yabancı olanlar sonradan yabancı olanlara göre operasyonel risk yönetiminde daha başarılıdır. Ancak, yabancı bankaların yabancılaşma süreleri ile bu bankaların operasyonel risk yönetimi arasındaki ilişki 0.25 olup oldukça zayıftır.

Tablo 53: Bankaların Yabancılaşma Süreleri ile Operasyonel Risk Yönetim Olgunluk Seviyeleri Arasındaki Korelasyon

		eskiyeni	genel
eskiyeni	Pearson Correlation	1	.246
	Sig. (2-tailed)		.282
	N	21	21
genel	Pearson Correlation	.246	1
	Sig. (2-tailed)	.282	
	N	21	21

Ancak, Pearson korelasyon katsayısı istatistiksel olarak anlamsızdır. Bunun iki sebebi olabilir

i) Gözlem sayısının azlığı.

ii) ii)Değişkenler arasındaki ilişkinin gerçekte doğrusal olmamasından kaynaklanabilir.

Bu durumda yapılması gereken Spearman korelasyon katsayısını hesaplamaktır. Tablo 54'de hesaplanan Spearman korelasyon katsayısı; yabancı bankaların yabancılaşma süreleri ile bu bankaların operasyonel risk yönetimi arasındaki ilişkinin pozitif yönlü olduğunu ve ilişkinin derecesinin 0.286 olup zayıf bir ilişki olduğunu gösterir. Spearman korelasyon katsayısı da (α=0.01< kuyruk olasılığı=0.208 olduğundan Spearman korelasyon katsayısı istatistiksel olarak anlamsızdır.) istatistiksel olarak anlamsızdır. Bu da ***yabancı bankaların yabancılaşma süreleri ile bu bankaların operasyonel risk yönetimi arasındaki ilişkinin gerçekte doğrusal olduğunu; fakat gözlem sayısının azlığından dolayı Pearson korelasyon katsayısının anlamsız çıktığını*** göstermektedir.

Tablo 54: Bankaların Yabancılaşma Süreleri ile Operasyonel Risk Yönetim Olgunluk Seviyeleri Arasındaki Eğrisel İlişki Korelasyonu

			eskiyeni	genel
Spearman's rho	eskiyeni	Correlation Coefficient	1.000	.286
		Sig. (2-tailed)	.	.208
		N	21	21
	genel	Correlation Coefficient	.286	1.000
		Sig. (2-tailed)	.208	.
		N	21	21

4.2.3.4. ORYOS Endeksinin Bankaların Yaşam Süreleri ile Korelasyonu

Uygulamada yapılan korelasyon analizinde bankaların kuruluşlarından bu yana geçen süre ile bu bankaların sahip oldukları operasyonel risk yönetimi olgunluk seviyesi arasındaki ilişki ölçülmüştür ve çıkan sonuçlar Tablo 55'de yer almaktadır.

Tablo 55: ORYOS Endeksinin Bankaların Yaşam Süreleri ile Korelasyonu

		bankayasi	genel
bankayasi	Pearson Correlation	1	.208
	Sig. (2-tailed)		.151
	N	49	49
genel	Pearson Correlation	.208	1
	Sig. (2-tailed)	.151	
	N	49	49

Pearson korelasyon katsayısına göre yorum yapıldığında çıkan değer yaklaşık 0.21 (%21) olduğu için bankanın yaşı ile operasyonel risk yönetimi performansının arasındaki ilişki pozitif olup güçlü bir ilişki söz konusu değildir. Ancak, Pearson korelasyon katsayısı, α=0.01 ve α=0.05 anlamlılık düzeylerinde istatistiksel olarak anlamsızdır.(α=0.01<kuyruk olasılığı=0.15 olduğundan Pearson korelasyon katsayısı istatistiksel olarak anlamsızdır.) Bu durum, bankaların kuruluşlarından bu yana geçen süre ile bu bankaların sahip oldukları operasyonel risk yönetimi olgunluk seviyeleri arasındaki ilişkinin doğrusal olmayabileceğini göstermektedir. Öyleyse, eğrisel ilişkiyi ölçen Tablo 56'da yer alan Spearman korelasyon katsayısına bakmalıyız.

Tablo 56: ORYOS Endeksinin Bankaların Yaşam Süreleri ile Eğrisel İlişki Korelasyonu

			bankayasi	genel
Spearman's rho	**bankayasi**	**Correlation Coefficient**	1.000	.271
		Sig. (2-tailed)	.	.060
		N	49	49
	genel	**Correlation Coefficient**	.271	1.000
		Sig. (2-tailed)	.060	.
		N	49	49

Ancak, Spearman korelasyon katsayısı da α=0.01 < kuyruk olasılığı=0.06 olduğundan, istatistiksel olarak anlamsızdır. Bu durumda, analizinde ***bankaların kuruluşlarından bu yana geçen süre ile bu bankaların sahip oldukları operasyonel risk yönetimi performansı arasındaki ilişkiyi ölçmek anlamsızdır***.

4.2.3.5. ORYOS Endeksinin Toplam Personel Sayısı ile Korelasyonu

Bankaların toplam personel sayısı ile ORYOS endeksi arasında ilişki incelendiğinde, Tablo 57'de yer alan pearson korelasyon katsayısına göre toplam personel sayısı ile operasyonel risk yönetimi olgunluk seviyesi arasında %33 oranında pozitif yönlü ancak çok güçlü olmayan bir ilişki söz konusudur.

Tablo 57: ORYOS Endeksinin Toplam Personel Sayısı ile Korelasyonu

		genel	toppersonal
genel	Pearson Correlation	1	.332*
	Sig. (2-tailed)		.020
	N	49	49
toppersonal	Pearson Correlation	.332*	1
	Sig. (2-tailed)	.020	
	N	49	49

*. Correlation is significant at the 0.05 level (2-tailed).

4.2.3.6. ORYOS Endeksinin Şube Sayısı ile Korelasyonu

Aşağıda yer alan Tablo 58'de Bankaların şube sayısı ile ORYOS endeksi arasındaki ilişki gösterilmektedir. Pearson korelasyon katsayısına göre bankaların şube sayıları ile operasyonel risk yönetimi performansı arasında %30 oranında pozitif ancak çok güçlü olmayan bir ilişki söz konusudur

Tablo 58: ORYOS Endeksinin Bankaların Şube Sayısı ile Korelasyonu

		genel	subesayisi
genel	Pearson Correlation	1	.303*
	Sig. (2-tailed)		.034
	N	49	49
subesayisi	Pearson Correlation	.303*	1
	Sig. (2-tailed)	.034	
	N	49	49

*. Correlation is significant at the 0.05 level (2-tailed).

.

4.2.4. Varyans Analizi

Varyans analizinde bağımlı ve bağımsız değişkenlerden bahsedilebilir. Bağımsız değişkenlere faktör adı da verilir. Faktörlerin bağımlı değişkenler üzerindeki etkisi araştırılır. Varyans analizi iki ya da daha fazla ortalama arasında fark olup olmadığı ile ilgili hipotezi test etmek için kullanılır. Hipotezler aşağıdaki gibidir:

H0:μ1= μ2=...= μn (Ortalamalardan en az ikisi arasında fark yoktur.)
H1:μ1≠ μ2≠... ≠ μn (Ortalamalardan en az ikisi arasında anlamlı fark vardır.)

Varyans analizi varsayımları[273];

- Bağımlı değişkene ait ölçümler en az eşit aralıklı ölçek düzeyinde olmalıdır.
- Ölçümler, bağımlı değişken üzerindeki etkisi araştırılan faktörün her bir düzeyinde normal dağılıma sahip olmalıdır.
- Örneklemler birbirinden bağımsız olmalıdır.
- Bağımlı değişkene ait varyanslar her bir örneklem için birbirine eşit olmalıdır.
- Bağımsız değişkenin kategorik,bağımlı değişkenin ise metrik olması gerekmektedir.

4.2.4.1. Faaliyet Türlerine Göre Bankalarla Yapılan Varyans Analizi

Yapılan çalışmada;

Bağımsız Değişken: Faaliyet açısından bankanın türü (mevduat, kalkınma&yatırım, katılım)

SPSS programında değişkenler 1-mevduat, 2-kalkınmayatırım, 3-katılım bankası olarak bağımsız değişkenler üç grupta toplanmıştır. Operasyonel risk yönetim olgunluk seviyesi faaliyet açısından bankanın türüne göre farklılık gösterip göstermediğini araştırmak için varyans analizi kullanılmalıdır.

Bağımlı Değişken: Operasyonel risk yönetim olgunluk seviyesi.

[273] Nuran Bayram, **Sosyal Bilimlerde SPSS ile Veri Analizi,** 1.Baskı, Bursa:Ezgi Kitabevi, 2004, s.99.

SPSS programında operasyonel risk yönetim olgunluk seviyesi ‘genel’ değişkeni ile ifade edilmiştir.

Çalışmada bir bağımlı değişken ve bir bağımsız değişken ile çalışıldığından tek yönlü varyans analizi yapılacaktır.

İlk olarak analizde kullanılan değişkenlerin tanımlayıcı istatistiklerine bakıldığında dikkati çeken örneklem sayıları ve ortalamalar Tablo 59’da yer almaktadır.

Tablo 59: Faaliyet Türlerine Göre Bankaların Tanımlayıcı İstatistikleri

genel

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
mevduat	32	3.0994	1.47933	.26151	2.5660	3.6327	.00	4.80
kalkinmayatirim	13	2.8015	1.48321	.41137	1.9052	3.6978	.00	4.90
katilim	4	3.0100	.11165	.05583	2.8323	3.1877	2.87	3.10
Total	49	3.0131	1.40755	.20108	2.6088	3.4174	.00	4.90

32 mevduat bankası, 13 kalkınma yatırım bankası ve 4 de katılım bankası bulunmaktadır. Mevduat bankalarının operasyonel risk yönetimi performansı ortalaması 3.09, kalkınma ve yatırım bankalarının operasyonel risk yönetimi olgunluk seviyesi ortalaması 2.80, katılım bankalarının operasyonel risk yönetimi olgunluk seviyesi ortalaması 3.01 dir. Varyans analizinde bu ortalamaların istatistiki açıdan farklılık yaratıp yaratmadığı incelenecektir.

Tek yönlü ANOVA’nın temel varsayımı olan varyansların homojenliğinin sağlanıp sağlanılmadığına aşağıdaki hipotezlerle bakılır;

H0: Varyans homojenliği sağlanmıştır.

H1: Varyans homojenliği sağlanmamıştır.

Tablo 60: Varyans Homojenliği Testi

genel

Levene Statistic	df1	df2	Sig.(p)
2.286	2	46	.113

Varyans homojenliği testi sonuçları Tablo 60'da yer almaktadır. Buradaki p değeri (sig.) 0,05'ten büyük olduğu için (0,113) varyansların homojen olduğu söylenir. Sonuç olarak varyans analizinin temel varsayımı sağlandığı için, varyans analizinden elde edilecek sonuçların sağlıklı olduğu söylenebilir.

Tablo 61'de faaliyet türlerine göre bankaların varyans analizine ilişkin sonuçlar yer almaktadır.

Tablo 61: Faaliyet Türlerine Göre Bankaların Varyans Analizi

genel

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.820	2	.410	.200	.819
Within Groups	94.278	46	2.050		
Total	95.098	48			

ANOVA tablosunda operasyonel risk yönetim olgunluk seviyesinin faaliyet açısından bankanın türüne göre farklılık gösterip göstermediği test edilmektedir. Hipotezler;

H0: μ1= μ2= μ3 (Faaliyet açısından gruplanan bankalar arasında operasyonel risk yönetimi olgunluk seviyelerinde anlamlı bir farklılık yoktur.)

H1: μ1≠ μ2≠ μ3 (Faaliyet açısından gruplanan bankalar arasında operasyonel risk yönetimi olgunluk seviyelerinde anlamlı bir farklılık vardır.)

Tablo 61'de sig. değeri (.8119)>(α=0.05) olduğundan H0 hipotezi reddedilemez. Yani faaliyet türlerine göre gruplanan bankalar arasında operasyonel risk yönetimi olgunluk seviyelerinde anlamlı bir farklılık olmadığı söylenir.

Sonuç olarak; bankaların faaliyetlerine göre operasyonel risk yönetimi olgunluk seviyesi ortalamaları arasında anlamlı bir farklılık olmadığı için bankaların mevduat, kalkınma yatırım ve katılım bankası olması operasyonel risk yönetimi olgunluk seviyesi açısından farklılık yaratmamaktadır. Yani bankaların operasyonel risk yönetim olgunluk seviyelerinin bankaların faaliyet türlerine göre değişiklik gösterdiği söylenemez. Diğer bir deyişle örneğin mevduat bankalarının kalkınma ve yatırım bankalarına göre veya katılım bankalarının kalkınma&yatırım ya da mevduat bankalarına göre operasyonel risk yönetimi olgunluk seviyelerinde bankanın türünün farklı olmasından dolayı bir fark vardır denemez.

Eğer gruplar arasında operasyonel risk yönetimi olgunluk seviyeleri açısından bir farklılık ortaya çıksaydı “Post Hoc” testleri ile ortaya çıkan farklılığın hangi gruplar arasında meydana geldiği araştırılacaktı.

4.2.4.2. Faktör Bazında Faaliyet Türlerine Göre Yapılan Varyans Analizi

Operasyonel risk yönetimi olgunluk seviyelerini etkileyen insan, sistem, süreç ve dışsal faktörlerin faaliyet türlerine göre gruplanan bankalar arasında farklılık oluşturup oluşturmayacağını operasyonel risk faktörleri için tek tek ancak aynı tablo üzerinde incelemek istediğimizde Tablo 62’de belirtilen sonuçlara ulaşılmaktadır:

Tablo 62: Dört Ana Faktör İçin Faaliyet Türlerine Göre Bankaların Tanımlayıcı İstatistikleri

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
insan	mevduat	32	3.2016	1.48890	.26320	2.6648	3.7384	.00	4.87
	kalkinmayatirim	13	2.7423	1.54075	.42733	1.8112	3.6734	.00	4.99
	katilim	4	2.9875	.42727	.21363	2.3076	3.6674	2.39	3.32
	Total	49	3.0622	1.44143	.20592	2.6482	3.4763	.00	4.99
sistem	mevduat	32	3.1166	1.51997	.26870	2.5686	3.6646	.00	5.02
	kalkinmayatirim	13	2.9792	1.49908	.41577	2.0733	3.8851	.00	4.93
	katilim	4	3.0875	.21329	.10664	2.7481	3.4269	2.89	3.39
	Total	49	3.0778	1.43540	.20506	2.6655	3.4900	.00	5.02
süreç	mevduat	32	2.9903	1.44285	.25506	2.4701	3.5105	.00	4.55
	kalkinmayatirim	13	2.5969	1.45213	.40275	1.7194	3.4744	.00	4.77
	katilim	4	2.7375	.36463	.18232	2.1573	3.3177	2.24	3.08
	Total	49	2.8653	1.38249	.19750	2.4682	3.2624	.00	4.77
d.faktorler	mevduat	32	3.0838	1.55457	.27481	2.5233	3.6442	.00	4.75
	kalkinmayatirim	13	2.8792	1.56113	.43298	1.9358	3.8226	.00	4.89
	katilim	4	3.2300	.22076	.11038	2.8787	3.5813	3.04	3.45
	Total	49	3.0414	1.47797	.21114	2.6169	3.4660	.00	4.89

İlk olarak tanımlayıcı istatistikler bulunmuştur. Daha sonra varyans analizinin temel varsayımı olan varyans homojenliği testi her bir operasyonel risk faktörü için yapıldığında Tablo 63'de yer alan sonuçlar alınmıştır.

Tablo 63: Dört Ana Faktör İçin Varyans Homojenliği Testi

	Levene Statistic	df1	df2	Sig.
İnsan	1.492	2	46	.236
Sistem	2.118	2	46	.132
Süreç	1.489	2	46	.236
d.faktorler	2.605	2	46	.085

H0: Varyans homojenliği sağlanmıştır.

H1: Varyans homojenliği sağlanmamıştır.

Tablo 63'de dört ana faktör için varyansların homojenliğine ilişkin H0, H1 hipotezleri test edilmiştir. Tablodaki dört ana faktör için sig. değerlerine bakıldığında; "İnsan" sig.=.236> α=0.05, "Sistem" sig.=.132>α=0.05, "Süreç" sig.=.236>α=0.05 ve "Dışsal Etkenler" sig.=.085> α=0.05 olduğu ve dört faktörün her birinin sig. değerlerinin α=0.05'ten büyük olduğu, bundan dolayı H0 hipotezinin reddedilemeyeceği görülür. Dolayısıyla tüm operasyonel risk yönetim faktörleri için varyans homojenliği sağlanmıştır. Artık dört ana faktör için ANOVA testi yapılabilir. Tablo 64'de bu testin sonuçları yer almaktadır.

Tablo 64: Dört Ana Faktör İçin Faaliyet Türlerine Göre Bankalarla Yapılan Varyans Analizi

		Sum of Squares	df	Mean Square	F	Sig.
insan	Between Groups	1.974	2	.987	.464	.631
	Within Groups	97.756	46	2.125		
	Total	99.730	48			
sistem	Between Groups	.175	2	.087	.041	.960
	Within Groups	98.723	46	2.146		
	Total	98.898	48			
süreç	Between Groups	1.502	2	.751	.383	.684
	Within Groups	90.239	46	1.962		
	Total	91.741	48			
d.faktorler	Between Groups	.542	2	.271	.119	.888
	Within Groups	104.309	46	2.268		
	Total	104.851	48			

Tablo 64'de her bir operasyonel risk yönetimi olgunluk seviyesi sig. değerlerine bakıldığında;

- **"İnsan" faktörü için;**

H0: İnsan kaynakları faktörü için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

H1: İnsan kaynakları faktörü için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmektedir.

İnsan kaynakları faktörü için 0.631>α=0.05 olduğu için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir. Yani örneğin mevduat bankalarının insan faktörüne yönelik operasyonel risk yönetim olgunluk seviyesinin diyelim kalkınma&yatırım bankalarının insan faktörüne ilişkin operasyonel risk yönetimi olgunluk seviyesine göre anlamlı bir farklılık göstermediği sonucuna ulaşılmaktadır.

- **“Sistem” faktörü için;**

H0: Sistem faktörü için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri ı arasında anlamlı bir farklılık görülmemektedir.

H1: Sistem faktörü için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri ı arasında anlamlı bir farklılık görülmektedir.

Sistem faktörü için 0.96>α=0.05 olduğu için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

- **“Süreç” faktörü için;**

H0: Süreç faktörü için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

H1: Süreç faktörü için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmektedir.

Süreç faktörü için 0.68>α=0.05 olduğu için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

- **“Dışsal Etkenler” faktörü için;**

H0: Dışsal faktörler için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

H1: Dışsal faktörler için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmektedir.

Dış etkenler faktörü için 0.88>α=0.05 olduğu için bankaların faaliyet türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

4.2.4.3. Sahiplik Türlerine Göre Bankalarla Yapılan Varyans Analizi

Operasyonel risk yönetimi olgunluk seviyesinin sahiplik açısından bankanın türlerine göre farklılık gösterip göstermediğini araştırmak için yapılacak varyans analizinde kullanılacak bağımsız değişkenler bu gruptaki banka türleri yani kamu, yerli özel ve yabancı bankalar olacaktır. SPSS programında değişkenler 1-kamu, 2-yabancı, 3-yerliözel banka olarak kategorik değişken haline getirilmiştir. Analizde kullanılacak bağımlı değişken ilgili banka gruplarının operasyonel risk yönetim olgunluk seviyesidir.

Çalışmada bir bağımlı değişken ve bir bağımsız değişken ile çalışıldığından tek yönlü varyans analizi yapılacaktır. Tablo 65'de analizde kullanılan değişkenlerin tanımlayıcı istatistikleri görülmektedir. Sahiplik açısından banka türleri; 8 kamu bankası, 21 yabancı banka ve 20 yerli özel banka olmak üzere üç gruba ayrılmaktadır.

Tablo 65: Sahiplik Türlerine Göre Bankaların Tanımlayıcı İstatistikleri

genel

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
kamu	8	2.7238	1.30234	.46045	1.6350	3.8125	.00	3.56
yabancý	21	3.2890	1.53829	.33568	2.5888	3.9893	.00	4.90
yerliözel	20	2.8390	1.31836	.29479	2.2220	3.4560	.00	4.33
Total	49	3.0131	1.40755	.20108	2.6088	3.4174	.00	4.90

Tablo 65'e göre, kamu bankalarının operasyonel risk yönetimi olgunluk seviyesi ortalaması (Mean) 2.72, yabancı bankaların operasyonel risk yönetimi olgunluk seviyesi ortalaması 3.29, yerli özel bankaların operasyonel risk yönetimi olgunluk seviyesi ortalaması 2.84'tür. Varyans analizinde bu ortalamaların istatistiki açıdan farklılık yaratıp yaratmadığı hususu incelenecektir.

Tek yönlü ANOVA'nın temel varsayımı olan varyansların homojenliğinin sağlanıp sağlanılmadığına Tablo 66'da bakılmıştır. İlgili hipotezler;

H0: Varyans homojenliği sağlanmıştır.

H1: Varyans homojenliği sağlanmamıştır.

Tablo 66: Sahiplik Türlerine Göre Bankaların Varyans Homojenliği Testi

genel

Levene Statistic	df1	df2	Sig.
.389	2	46	.680

Tablo 66'daki p değeri (sig.) .680>α=0.05 olduğu için H0 hipotezi, yani varyansların homojen olduğu kabul edilir. Sonuç olarak varyans analizinin temel varsayımı sağlandığı için, varyans analizinden elde edilecek sonuçların sağlıklı olduğu söylenebilir. Artık varyans analizine geçilebilir.

Yapılan varyans analizi sonuçları Tablo 67'de belirtilmektedir. ANOVA tablosunda operasyonel risk yönetim olgunluk seviyesinin sahiplik açısından bankanın türüne göre farklılık gösterip göstermediği test edilmektedir. Hipotezler;

H0: μ1= μ2= μ3 (Sahiplik açısından gruplanan bankaların operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık yoktur.)

H1: μ1≠ μ2≠ μ3 (Sahiplik açısından gruplanan bankaların operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık vardır.)

Tablo 67: Sahiplik Türlerine Göre Bankaların Varyans Analizi

genel

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.875	2	1.438	.717	.494
Within Groups	92.223	46	2.005		
Total	95.098	48			

Tablo 67'de sig. değeri .494>α=0.05'ten büyük olduğundan H0 hipotezi reddedilemez ve dolayısıyla sahiplik türlerine göre gruplanan bankaların operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık olmadığı söylenebilir.

Sonuç olarak; bankaların sahipliklerine göre operasyonel risk yönetimi olgunluk seviyeleri arasında anlamlı bir farklılık olmadığı için bankaların kamu, yabancı veya yerli

özel banka olması operasyonel risk yönetimi olgunluk seviyesi açısından farklılık yaratmamaktadır.

4.2.4.4. Faktör Bazında Sahiplik Türlerine Göre Yapılan Varyans Analizi

Operasyonel risk yönetim olgunluk seviyesini etkileyen insan, sistem, süreç ve dışsal etkenlerin bankaların sahiplik türlerine göre gruplanan bankalar arasında farklılık oluşturup oluşturmayacağı operasyonel risk faktörleri için tek tek ancak aynı tablo üzerinde incelenmek istendiğinde Tablo 68'de yer alan sonuçlara ulaşılmaktadır:

Tablo 68: Dört Ana Faktör İçin Sahiplik Türlerine Göre Bankaların Tanımlayıcı İstatistikleri

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
insan	kamu	8	2.6325	1.37316	.48548	1.4845	3.7805	.00	3.75
	yabancý	21	3.3629	1.54071	.33621	2.6615	4.0642	.00	4.99
	yerliözel	20	2.9185	1.36241	.30464	2.2809	3.5561	.00	4.33
	Total	49	3.0622	1.44143	.20592	2.6482	3.4763	.00	4.99
sistem	kamu	8	2.8888	1.31709	.46566	1.7876	3.9899	.00	3.76
	yabancý	21	3.2814	1.56205	.34087	2.5704	3.9925	.00	5.02
	yerliözel	20	2.9395	1.38441	.30956	2.2916	3.5874	.00	4.67
	Total	49	3.0778	1.43540	.20506	2.6655	3.4900	.00	5.02
süreç	kamu	8	2.5875	1.26445	.44705	1.5304	3.6446	.00	3.69
	yabancý	21	3.1862	1.49861	.32702	2.5040	3.8683	.00	4.77
	yerliözel	20	2.6395	1.29438	.28943	2.0337	3.2453	.00	4.32
	Total	49	2.8653	1.38249	.19750	2.4682	3.2624	.00	4.77
d.faktorler	kamu	8	2.7788	1.39710	.49395	1.6107	3.9468	.00	3.74
	yabancý	21	3.3214	1.61629	.35270	2.5857	4.0572	.00	4.89
	yerliözel	20	2.8525	1.37701	.30791	2.2080	3.4970	.00	4.25
	Total	49	3.0414	1.47797	.21114	2.6169	3.4660	.00	4.89

Tablo 68'de öncelikle tanımlayıcı istatistikler bulunmuştur. Aşağıda Tablo 69'da varyans analizinin temel varsayımı olan varyans homojenliği testi her bir operasyonel risk faktörü için yapılmıştır.

H0: Varyans homojenliği sağlanmıştır.

H1: Varyans homojenliği sağlanmamıştır.

Tablo 69'da dört ana faktör için varyansların homojenliğine ilişkin H0, H1 hipotezleri test edilmiştir. Tablodaki dört ana faktör için sig. değerlerine bakıldığında; "İnsan" sig.=.845> α=0.05, "Sistem" sig.=.706>α=0.05, "Süreç" sig.=.707>α=0.05 ve

“Dışsal Etkenler” sig.=.620> α=0.05 olduğu ve dört faktörün her birinin sig. değerlerinin α=0.05’ten büyük olduğu, bundan dolayı H0 hipotezinin reddedilemeyeceği görülür.

Tablo 69: Dört Ana Faktör İçin Varyans Homojenliği Testi

	Levene Statistic	df1	df2	Sig.
insan	.169	2	46	.845
sistem	.350	2	46	.706
süreç	.349	2	46	.707
d.faktorler	.483	2	46	.620

Dolayısıyla tüm operasyonel risk yönetim faktörleri için varyans homojenliği sağlanmıştır. Artık dört ana faktör için ANOVA testi yapılabilir. Bu testin sonuçları Tablo 70’de yer almaktadır.

Tablo 70: Dört Ana Faktör İçin Sahiplik Türlerine Göre Bankalarla Yapılan Varyans Analizi (ANOVA)

		Sum of Squares	df	Mean Square	F	Sig.
insan	Between Groups	3.788	2	1.894	.908	.410
	Within Groups	95.942	46	2.086		
	Total	99.730	48			
sistem	Between Groups	1.539	2	.770	.364	.697
	Within Groups	97.358	46	2.116		
	Total	98.898	48			
süreç	Between Groups	3.799	2	1.900	.994	.378
	Within Groups	87.942	46	1.912		
	Total	91.741	48			
d.faktorler	Between Groups	2.912	2	1.456	.657	.523
	Within Groups	101.938	46	2.216		
	Total	104.851	48			

Tablo 70’deki her bir operasyonel risk yönetimi olgunluk seviyesi sig. değerlerine bakıldığında;

- **“İnsan” faktörü için;**

H0: İnsan kaynakları faktörü için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

H1: İnsan kaynakları faktörü için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmektedir.

İnsan kaynakları faktörü için 0.41>α=0.05 olduğu için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir. Yani örneğin kamu bankalarının insan faktörüne yönelik operasyonel risk yönetim olgunluk seviyesinin diyelim yabancı bankalarının insan faktörüne ilişkin operasyonel risk yönetimi olgunluk seviyesine göre anlamlı bir farklılık göstermediği sonucuna ulaşılmaktadır.

- **“Sistem” faktörü için;**

H0: Sistem faktörü için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri ı arasında anlamlı bir farklılık görülmemektedir.

H1: Sistem faktörü için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri ı arasında anlamlı bir farklılık görülmektedir.

Sistem faktörü için 0.697>α=0.05 olduğu için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

- **“Süreç” faktörü için;**

H0: Süreç faktörü için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

H1: Süreç faktörü için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmektedir.

Süreç faktörü için 0.378>α=0.05 olduğu için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

- **“Dışsal Etkenler” faktörü için;**

H0: Dışsal faktörler için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

H1: Dışsal faktörler için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmektedir.

Dış etkenler faktörü için 0.523>α=0.05 olduğu için bankaların sahiplik türlerine göre operasyonel risk yönetim olgunluk seviyeleri arasında anlamlı bir farklılık görülmemektedir.

4.2.5. Kümeleme Analizi

"Segment analizi" ve "taksonomi analizi" olarak da adlandırılan[274] çok değişkenli bir analiz türü olan kümeleme analizinin temel amacı n sayıda gözlemi, p sayıda değişkene göre saptanan özelliklere uygun olarak kendi içinde türdeş(homojen) ve kendi aralarında farklı (heterojen) alt gruplara (küme) ayırmaktır[275]. Yani, bir kümeyi oluşturan bireyler birbirleriyle benzeşirken, diğer kümelerin bireyleriyle benzeşmeyecektir.

Bankaların operasyonel risk yönetim performansı açısından değerlendirilebilmesi için kümeleme analizi yapılmıştır. Kümeleme analiziyle bankalar operasyonel risk yönetim performansı açısından kümelere ayrılmıştır.

Tablo 71 "İlk Küme Merkezleri" olarak isimlendirilmekte ve bu tabloda her kümenin ilgili değişken itibariyle merkezi gösterilmektedir.

Tablo 71: İlk Küme Merkezleri

	Cluster		
	1	2	3
insan	2.93	.00	4.99
sistem	2.64	.00	4.93
süreç	2.12	.00	4.77
dissal	2.47	.00	4.89
genel	2.54	.00	4.90

Tablo 72, tekrarlama sayısını vermektedir. Analizde en fazla 10 kez tekrarlama önerilmiş, fakat program 3 kez tekrarlamada 3 kümeyi oluşturmuştur. Böylece tekrarlamanın 10 kez yapılmasına gerek kalmamıştır.

[274] Hüseyin Tatlıdil, **Uygulamalı Çok Değişkenli İstatistiksel Analiz**, Ankara:Akademi Matbaası, 2002, s.55.
[275] Kazım Özdamar, **Paket Programlar İle İstatistiksel Veri Analizi (Çok Değişkenli Analizler)**, 4.Baskı, Eskişehir:Kaan Kitabevi, 2002, s.279.

Tablo 72: Küme Analizinde Tekrarlama Sayısı

Iteration	Change in Cluster Centers		
	1	2	3
1	1.249	.000	1.496
2	.147	.409	.000
3	.000	.000	.000

a Convergence achieved due to no or small change in cluster centers. The maximum absolute coordinate change for any center is .000. The current iteration is 3. The minimum distance between initial centers is 5.285.

Tablo 73 küme üyeliğini göstermektedir. Küme üyeliği hiyerarşik olmayan kümelemede en önemli çıktıdır. Burada hangi gözlemin hangi kümenin üyesi olduğu belirlenir. Her gözlemin mensubu bulunduğu kümeden uzaklığını da bu tabloda bulmak mümkündür.

Tablo 73: Küme Üyeliği

Case Number	banka	Cluster	Distance
1	B01	1	.491
2	B02	1	.834
3	B03	1	.998
4	B04	2	.409
5	B05	3	.899
6	B06	1	1.458
7	B07	3	.706
8	B08	3	.467
9	B09	3	.209
10	B10	3	1.296
11	B11	1	1.957
12	B12	3	.481
13	B13	2	.409
14	B14	3	.745
15	B15	2	.409
16	B16	1	.978
17	B17	3	.558
18	B18	3	.614
19	B19	3	.364
20	B20	1	1.955
21	B21	1	.422

22	B22	3	.400
23	B23	3	.515
24	B24	3	.814
25	B25	3	.812
26	B26	1	1.153
27	B27	1	.767
28	B28	1	1.789
29	B29	1	.633
30	B30	1	.777
31	B31	2	.409
32	B32	2	.409
33	B33	1	1.340
34	B34	1	.995
35	B35	1	.917
36	B36	2	2.865
37	B37	1	.645
38	B38	3	.356
39	B39	3	1.496
40	B40	2	.409
41	B41	1	1.037
42	B42	2	.409
43	B43	1	1.251
44	B44	1	1.385
45	B45	1	.901
46	B46	1	.947
47	B47	1	.287
48	B48	1	.444
49	B49	1	.818

Bu aşamada Tablo 73'den önemli sentezler çıkarabilir. Mesela, her kümenin elemanlarını alt alta koyarak ve ortak özelliklerini gözleyerek, bu kümedeki gözlemlere bir isim takılabilir.

- B01 ,B02, B03, B06 , B11, B20, B21, B16, B26, B27, B28, B29 ,B30 ,B33, B34, B35, B37,B41, B43 ,B44, B45, B46, B47 ,B48, B49 bankaları operasyonel risk yönetim performansı açısından aynı grupta yer almakta olup **1. kümede** bulunmaktadırlar,

- B04, B13, B15, B22 ,B32, B36 ,B40, B42 bankaları ise operasyonel risk yönetimi açısından aynı grupta yer almakta olup **2.kümede** bulunmaktadırlar,

- B05, B07, B08, B09, B10, B12, B14 ,B17, B18, B19, B22, B23, B24, B25,B38 ve B39 Bankaları ise, aynı grupta yer alıp **3.kümede** bulunmaktadırlar.

Tablo 74**'**de yer alan "Final Küme Merkezleri" çok önemli bir çıktıdır. Burada insan,sistem,süreç ve dışsal faktörler ile operasyonel risk yönetim olgunluk seviyesi değişkenlerinin üç kümedeki ortalamaları verilmiştir.

Tablo 74: Final Küme Merkezleri

	Cluster		
	1	2	3
insan	3.25	.15	4.22
sistem	3.22	.23	4.27
süreç	2.92	.18	4.12
dışşal	3.16	.16	4.30
genel	3.14	.18	4.23

Final küme merkezlerine bakıldığında 3.küme; "insan", "sistem", "süreç" ve "dışsal faktörlere" en fazla önemi veren ve operasyonel risk yönetimi açısından en başarılı olan kümedir. 1.küme ise 3.kümeden sonra operasyonel risk yönetiminde en başarılı 2.kümedir. B05,B07, B08, B09, B10, B12, B14 ,B17 , B18,B19,B22,B23,B24,B25,B38 ve B39 bankaları 3.kümede yer alan bankalar iken; B01 ,B02, B03, B06 , B11, B20, B21, B16, B26, B27, B28, B29 ,B30 ,B33, B34, B35, B37,B41, B43 ,B44, B45, B46, B47 ,B48, B49 bankaları operasyonel risk yönetim olgunluk seviyesi açısından aynı grupta yer almakta olup 1.kümede bulunmaktadırlar.

Final Küme Merkezleri Arasındaki Mesafeler: Kümeleme analizinde bulunan kümelerin birbirlerine yakın veya uzak olmaları, analiz sonucunda bulunan grupların

sıralanmasında önemlidir. Tablo 75 oluşan en son küme merkezleri arasındaki uzaklıkları göstermekte diğer bir deyişle hangi kümenin bir diğerinden ne kadar uzak olduğunu göstermektedir. Bu tablo çok sayıda küme söz konusu olduğunda daha çok önem kazanmaktadır.

Tablo 75: Final Küme Merkezleri Arasındaki Mesafeler

Cluster	1	2	3
1		6.619	2.445
2	6.619		9.054
3	2.445	9.054	

Kümeleme analizi neticesinde oluşan 3 farklı küme, tablonun satır ve sütunlarına yazılarak birbirleriyle ikili karşılaştırmalara tabi tutulmuş ve kesişim noktalarına ilgili iki kümenin birbirinden uzaklıkları yazılmıştır. Örneğin;

- Tablonun 1.satırında bulunan 1.kümenin tablonun 3.sütununda bulunan 3.kümeye uzaklığı 2.445'dir.
- Tablonun 1.satırında bulunan 1.kümenin tablonun 2.sütununda bulunan 2.kümeye uzaklığı 6.619'dur.
- Tablonun 2.satırında bulunan 2.kümenin tablonun 3.sütununda bulunan 3.kümeye uzaklığı 9.054'dür.

Kümeler arasındaki bu uzaklık değerlerine bakıldığında, en çok 1. kümeyle 3. kümenin birbirine yakın olduğunu, diğer taraftan da en fazla 2.kümeyle 3.kümenin birbirinden uzak olduğu söylenebilir.

Sonuçlar operasyonel risk yönetim olgunluk seviyesi açısından yorumlandığında; 3.kümede yer alan bankaların operasyonel risk yönetim olgunluk seviyelerinin 1.kümede yer alan bankaların operasyonel risk yönetim olgunluk seviyelerine yakın olduğu söylenebilmektedir. Diğer taraftan 2.kümede yer alan bankaların operasyonel risk yönetim olgunluk seviyesinin 3.kümedekilere göre en uzak olduğu söylenebilir. Yukarıdaki final küme merkezleri tablosundan da 3.kümede yer alan bankaların operasyonel risk yönetim

olgunluk seviyelerinin en başarılı olduğu sonucu çıkmıştı. Bu durumda 3.kümede yer alan bankalar operasyonel risk yönetimi açısından en başarılı küme olup 2.kümede yer alan bankalar operasyonel risk yönetimi performansı açısından diğer iki kümeye nispeten en başarısız kümedir. Dolayısıyla, 2.küme ile 3.küme arasındaki uzaklık operasyonel risk yönetim olgunluk seviyesi açısından en fazladır.

Tablo 76'da kümelerdeki birim sayısı gösterilmektedir. Kümelerdeki birim sayısı her kümede kaç birimin olduğunu gösterdiğinden önemlidir. Kuşkusuz ki her kümeye düşen birim sayısının eşit olması şart değildir. Ancak, sayılar arasında büyük farklar olması da arzulanan bir durum değildir. Çalışmada yer alan kümelerin birim sayısı makul sayılabilir.

Tablo 76: Kümelerdeki Birim Sayısı

Cluster	1	25.000
	2	8.000
	3	16.000
Valid		49.000
Missing		.000

Kümeleme analizine göre ayrılan banka gruplarının ORYOS endeks aralıkları Tablo 77'de yer almaktadır. ORYOS endeks değerleri anket sonuçlarından elde edilen verilerin istatistiki analize tabi tutulması sonucu elde edilmiş olup tablonun en sağ sütununda yer alan ORYOS sermaye yükümlülük çarpanları ORYOS endeksleri ile ters orantılı olacak şekilde 0 ila 1 arasındaki sayılardan üretilmiş olup, belli bir kritere dayanmamaktadır.

Tablo 77: Kümelerin ORYOS Endeks Aralığı ve Örnek ORYOS Sermaye Yükümlülük Çarpanları

ORYOS ENDEKS ARALIĞI	BANKA GRUBU	ORYOS Sermaye Yükümlülük Çarpanı
3.62 - 5.00	3.Küme	0.40
2.27 - 3.61	1.Küme	0.75
0.01 - 2.26	2.Küme	0.90

4.3. Anket Sonuçlarına Göre ORYOS Endekslerinin Hesaplanması

Anket sonuçlarına göre oluşturulan ORYOS endeksleri Tablo 78'de yer almaktadır. Söz konusu endeksler münferit olarak her banka için ayrı ayrı hesaplanabileceği gibi sahiplik veya faaliyet açısından gruplanan bankalar için de hesaplanabilir. Çalışmamızda bankalardan alınan verilerin gizliliği nedeniyle münferit banka bazında hesaplanan ORYOS endeksleri gizli tutulmuş olup açıklanmayacaktır. Aşağıdaki tabloda sadece banka gruplarını ve sektörü temsil eden 14 farklı ORYOS endeksi yer almaktadır. Ayrıca oluşturulan 14 farklı endeksin her biri için operasyonel riski tanımlayan dört ana faktör için de dört ayrı endeks hesaplanmıştır. Dolayısıyla çalışma sonucunda 14 farklı kategoride ve dört ana faktör altında hesaplanan endekslerle beraber toplam 70 adet endeks oluşturulmuştur.

Tablo 78: Anket Sonuçlarına Göre Hesaplanan ORYOS Endeksleri

ENDEKSLER	$ORYOS_{genel}$	$ORYOS_{insan}$	$ORYOS_{sistem}$	$ORYOS_{süreç}$	$ORYOS_{dışsal}$
$ORYOS_{kamu}$	3.11	3.01	3.30	2.96	3.18
$ORYOS_{yerli\text{-}özel}$	3.34	3.43	3.46	3.11	3.36
$ORYOS_{yabancı}$	3.84	3.92	3.83	3.72	3.88
$ORYOS_{mevduat}$	3.67	3.79	3.69	3.54	3.65
$ORYOS_{kalk\&yat}$	3.31	3.24	3.52	3.07	3.40
$ORYOS_{katılım}$	3.01	2.99	3.09	2.74	3.23
$ORYOS_{kamu\text{-}mevduat}$	3.47	3.49	3.40	3.34	3.62
$ORYOS_{kamu\text{-}kalk\&yatırım}$	2.85	2.65	3.23	2.67	2.84
$ORYOS_{yerliözel\text{-}mevduat}$	3.58	3.78	3.67	3.44	3.44
$ORYOS_{yerliözel\text{-}kalk\&yatırım}$	3.12	3.10	3.35	2.73	3.30
$ORYOS_{yerliözel\text{-}katılım}$	3.01	2.99	3.09	2.74	3.23
$ORYOS_{yabancı\text{-}mevduat}$	3.77	3.86	3.77	3.65	3.79
$ORYOS_{yabancı\text{-}kalk\&yatırım}$	4.18	4.22	4.14	4.06	4.29
$ORYOS_{sektör}$	3.52	3.57	3.59	3.34	3.55

4.4. ORYOS Sermaye Yükümlülük Çarpanının Sermaye Yeterliliği Standart Oranı Hesabında Kullanılması

Çalışma neticesinde ankete katılan her banka için belirlenen dört ana faktöre ait ORYOS ile bankacılık sektörü veya çeşitli kriterlere göre sınıflanan banka grupları için belirlenen operasyonel risk yönetimi olgunluk seviyeleri gerek ilgili kurumlar gerekse düzenleyici otorite tarafından bir endeks niteliğinde kullanılabilir.

Bu çalışma gerek münferit olarak ilgili banka bünyesinde gerekse de düzenleyici otoritenin tavsiyesi veya zorunluluğuyla periyodik olarak, örneğin yılda bir veya iki yılda bir tüm bankacılık sektörü için tekrarlanarak o döneme ilişkin operasyonel risk yönetim olgunluk seviyesi hesaplanıp, bunlar önceki dönemlerde alınan puanlarla karşılaştırılabilir. Böylece gerek düzenleyici otorite gerekse de münferiden her banka kendisinin ve sektörün operasyonel risk yönetim seviyesi hakkında rahatlıkla fikir sahibi olabilir, duruma göre çeşitli aksiyonlar alabilir. Bankalar hesaplanan endekslerle kendi durumunun sektör içerisindeki düzeyini karşılaştırabilir, kendi bünyesindeki operasyonel risk yönetim noktalarındaki gelişmeleri izleyebilir.

Bu uygulama hatta biraz daha ileriye giderek Basel-II çerçevesinde operasyonel risk ölçümünde gelişmiş ölçüm yöntemlerini kullanamayan veya kullanmak istemeyen bankalar için temel gösterge ve standart yaklaşıma yeni bir bakış açısı getirebilir. Örneğin temel gösterge yaklaşımında, bankanın son üç yıl itibariyle gerçekleşen yıl sonu brüt gelir tutarının %15'inin ortalamasının 12.5 ile çarpılması suretiyle bulunacak değer, *"operasyonel riske esas tutar"* olarak yani sermaye yeterliliği standart oranının hesabında kesrin paydasında yer alan ve operasyonel risk nedeniyle maruz kalınabilecek zararlara karşı bulundurulması gereken özkaynak miktarının tespitinde dikkate alınan tutardır. Basel Komitesi temel gösterge yaklaşımında operasyonel riske esas tutarın hesaplanışında basit bir yaklaşım sergilemiş ve son üç yılın brüt gelir ortalamasının %15 gibi standart bir oranını dikkate alarak bunu 12.5 ile çarpmıştır. Çalışmamızda münferit olarak her banka veya sahiplik ve faaliyet açısından farklılık gösteren banka grupları için 14 farklı ORYOS endeksi bulunmuştur. Düzenleyici otorite mesela bankaları sahip oldukları ORYOS endeksi puanına göre sınıflandırabilir ve her grup için ORYOS endeksi ile ters orantılı ORYOS sermaye yükümlülük çarpanı bulabilir. Bu çarpan örneğin 0 ila 1 arasında değişen bir sayı olarak ORYOS endeksi yükseldikçe sıfıra yaklaşan, ORYOS endeksi düştükçe 1'e

yaklaşan bir çarpan olabilir. Böylece bankalar için hesaplanacak sermaye yükümlülüğünde, yapılacak operasyonel riske esas tutar hesabında bankaların ORYOS endeksi puanına göre ilgili ORYOS sermaye yükümlülük çarpanı kullanılabilir.

Örneğin çalışmamızın istatistiki analiz bölümünde bankaların ankete verdikleri cevaplar ve bu cevapların AHS yöntemiyle yapılan ağırlıklandırılması neticesinde her bir bankanın ORYOS endeksi hesaplanmış ve sektördeki tüm bankalar için elde edilen sonuçlar kümeleme analizine tabi tutulmuştur. Söz konusu analiz neticesinde sektördeki bankalar ORYOS endeksi açısından 3 farklı kümeye ayrılmıştır. İstatistiki olarak ORYOS endeksine göre üçe ayrılan bu grupların her biri için ORYOS endeksi sermaye yükümlülük çarpanı tespit edilebilir ve bu çarpan bankalar için hesaplanacak sermaye yükümlülük oranı hesabında dikkate alınabilir.

Yukarıda anlatılanlar şu şekilde örneklendirilebilir;

Sektörde faaliyet gösteren büyük ve orta ölçekli 6 bankanın 2008 yılı faaliyet raporlarında yer alan sermaye yeterliliği standart oranına ilişkin özet bilgilerden faydalanılarak riske esas tutar içerisindeki kredi riskine esas tutarın, piyasa riskine esas tutarın ve operasyonel riske esas tutarın payları hesaplanmış ve aşağıdaki örnekte yer alan A,B,C Bank'ın verilerine oransal açıdan esas teşkil etmiştir.

Tablo 79'da yer alan değerlere göre operasyonel riskler için temel gösterge yaklaşımı ile söz konusu 3 banka için sermaye yeterlilik standart oranı hesaplanacak, ardından aynı hesaplama ORYOS sermaye yükümlülük çarpanları da hesaplamanın içine dahil edilerek yeniden yapılacaktır. Örnekte A-Bank ve B-Bank'ın hesaplamaya tabi değerleri bilerek aynı seçilmiştir. Amaç her iki bankanın ORYOS endeks puanları arasındaki farkın sonucu nasıl değiştirdiğini göstermektir.

Tablo 79: A,B,C Bankaları İçin Yapılan Sermaye Yeterlilik Hesabı

AÇIKLAMA	A-BANK	B-BANK	C-BANK
Operasyonel Riske Esas Tutar	5,000,000	5,000,000	4,000,000
Kredi Riskine Esas Tutar	43,000,000	43,000,000	30,000,000
Piyasa Riskine Esas Tutar	2,000,000	2,000,000	1,900,000
Toplam Riske Esas Tutar	50,000,000	50,000,000	35,900,000
Özkaynak Tutarı	3,850,000	3,850,000	2,850,000
Sermeye Yeterlilik Oranı	**%7.70**	**%7.70**	**%7.94**

Tablo 79'da örnekteki 3 banka için temel gösterge yaklaşımına göre sermaye yeterlilik standart oranı hesaplanmıştır. Bu hesaplamada A ve B Bankaları için hesaplanan oranın %7.70 ile aynı olduğu dikkat çekmektedir. C Bankasının oranı ise %7.94'tür. Bu haliyle 3 banka da tutturulması ve idamesi şart olan asgari %8 sermaye yeterliliği standart oranını tutturamamıştır.

Tablo 80'de sermaye yeterliliği standart oranının hesaplanması sürecine ORYOS endeksine bağlı olarak tespit edilen ORYOS sermaye yükümlülük çarpanları da dahil edilmiştir. Buna göre ORYOS endeks puanı diğer iki bankaya göre yüksek olan (Küme analizine göre en iyi grupta yer alan banka) A-Bank'ın ORYOS sermaye yükümlülük çarpanı 0.40, ORYOS endeks puanı diğerlerine göre en düşük olan C-Bank'ın ORYOS sermaye yükümlülük çarpanı 0.90 olarak belirlenmiştir. B-Bank ise bu iki bankanın ortasında yer alıp ORYOS sermaye yükümlülük çarpanı 0.75'dir.

Burada dikkat çeken husus A ve B-Bank'ın ORYOS endeks puanları ve dolayısıyla ORYOS sermaye yükümlülük çarpanları haricindeki bütün sayısal değerlerinin aynı olmasıdır. Yapılan hesaplamada Bankaların temel gösterge yaklaşımına göre bulunan operasyonel riske esas tutarları, çalışmanın temel önerisi olarak sunulan ORYOS endeksine göre belirlenmiş ORYOS sermaye yükümlülük çarpanları ile de çarpılarak yeniden her banka için bir ORYOS çarpanlı operasyonel riske esas tutar hesaplanmıştır.

Tablo 80: ORYOS Sermaye Yükümlülük Çarpanı Kullanılarak A,B,C Bank İçin Yapılan Sermaye Yeterlilik Hesabı

AÇIKLAMA	A-BANK	B-BANK	C-BANK
Operasyonel Riske Esas Tutar (ORET)	5,000,000	5,000,000	4,000,000
ORYOS Sermaye Yükümlülük Çarpanı	0.40	0.75	0.90
ORYOS Çarpanlı ORET	**2,000,000**	**3,750,000**	**3,600,000**
Kredi Riskine Esas Tutar	43,000,000	43,000,000	30,000,000
Piyasa Riskine Esas Tutar	2,000,000	2,000,000	1,900,000
Toplam Riske Esas Tutar	47,000,000	48,750,000	35,500,000
Özkaynak Tutarı	3,850,000	3,850,000	2,850,000
Sermeye Yeterlilik Oranı	**%8.19**	**%7.90**	**%8.03**

Tablo 80'den de görüleceği üzere ORYOS endeks puanı yüksek olan bankanın ORYOS sermaye yükümlülük çarpanı düşük olduğundan, sermaye yeterlilik standart oranının paydasını oluşturan operasyonel riske esas tutar değerini aşağı çekmekte ve böylece bankanın sermaye yeterlilik standart oranını yükseltmektedir. Gerçekten de örneğe bakıldığında A ve B Bank'ın ORYOS endeks puanları haricinde diğer tüm değerleri aynı olmasına rağmen ORYOS sermaye yükümlülük çarpanı ile sermaye yeterlilik standart oranı A-Bank için %8.19 hesaplanmış, B-Bank için ise ORYOS endeksinin düşüklüğüne bağlı olarak oran tutturulması gereken %8'lik asgari seviyenin altında %7.90 'da kalmıştır. Aynı şekilde C-Bank'da ORYOS endeksindeki kötü performansa rağmen sınırda da olsa %8.03 ile asgari oranı tutturabilmiştir.

Tablo 81'in ilk satırında örnekteki üç bankanın da sermaye yeterliliği standart oranını (%8) tutturması için gerekli olan sermaye gereksinimi tutarları yer almaktadır. Buna göre A-Bank 150,000.-TL, B-Bank 150,000.-TL ve C-Bank 22,000.-TL tutarında sermaye yeterlilik standart oranının payında yer alan özkaynak tanımına uygun nitelikte sermayeyi hesaplama döneminden itibaren altı ayı geçmemek üzere tamamlamak zorundadır[276]. Aynı tablonun ikinci satırında ise çalışmada açıklanan ORYOS endeksine göre belirlenen

[276] BDDK, "Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik", 01/11/2006 tarih ve 26333 sayılı Resmi Gazete, (Md:21).

ORYOS sermaye yükümlülük çarpanı ile bankaların operasyonel riske esas tutarlarının düzeltilmesi sonucunda hesaplanan sermaye yeterlilik standart oranına göre (%8) fazla veya eksik olan özkaynak tutarları gösterilmektedir.

Tablo 81: ORYOS Sermaye Yükümlülük Çarpanı Kullanılarak A,B,C Bank İçin Yapılan Sermaye Yeterlilik Hesabı

AÇIKLAMA	A-BANK	B-BANK	C-BANK
(ORYOS Öncesi) %8'lik Sermaye Yeterlilik Oranına Göre Hesaplanan Sermaye Gereksinimi	150,000	150,000	22,000
(ORYOS Sonrası) %8'lik Sermaye Yeterlilik Oranına Göre Hesaplanan Sermaye Gereksinimi	-90,000	50,000	-10,000

Buna göre mevcut uygulama doğrultusunda A-Bank'ın sermaye yeterliliği standart oranını tutturması için 150,000.-TL tutarında ek özkaynak gereksinimi varken, operasyonel riske esas tutarın ORYOS sermaye yükümlülük oranı çarpanı ile düzeltilmesi sonucunda sermaye gereksinimi ortadan kalktığı gibi 90,000.-TL tutarında bir özkaynak fazlalığı da ortaya çıkmaktadır. Aynı şekilde B-Bank'ın yürürlükteki mevzuata göre özkaynak gereksinimi 150,000.-TL iken operasyonel riske esas tutarın ORYOS sermaye yükümlülük oranı çarpanı ile düzeltilmesi sonucunda bu gereksinim 100,000.-TL azalarak 50,000.-TL'ye düşmüştür. C-Bank için hesaplanan sermaye yeterlilik standart oranına göre ortaya çıkan sermaye gereksinimi 22,000.-TL iken bu tutar operasyonel riske esas tutarın ORYOS sermaye yükümlülük oranı çarpanı ile düzeltilmesi sonucunda 10,000.-TL özkaynak fazlasına dönüşmüştür.

Sonuç olarak Basel yaklaşımına göre düzenleyici otoritenin emrettiği şekilde temel gösterge yaklaşımına göre yukarıdaki üç banka için hesaplanan sermaye yeterlilik standart oranları % 8'in altında kalmış, ancak çalışmanın önerisi olarak bankaların ölçülen ORYOS endeksine göre belirlenmiş olan ORYOS sermaye yükümlülük çarpanına göre hesaplanan

sermaye yeterlilik standart oranları A ve C-Bank için %8'lik asgari düzeyini geçebilmişlerdir.

Çalışmanın bu kısmında verilen örnek ORYOS endeksine bağlı olarak belirlenen ORYOS sermaye yükümlülük çarpanının temel gösterge yaklaşımı baz alınarak hesaplanan sermaye yeterliliği standart oranının hesabında bir düzeltme katsayısı olarak kullanılmasıdır. ORYOS endeksi ve çarpanının aynı şekilde standart yaklaşıma veya alternatif standart yaklaşıma göre hesaplanan sermaye yeterliliği standart oranının bankaların operasyonel risk yönetimi olgunluk seviyelerini göz önüne alan bir düzeltme katsayısı ile hesaplanması en az temel gösterge yaklaşımı kadar kolay ve anlaşılırdır. Bu sebeple ilgili husus tekraren bu konular için örneklendirilmemiştir.

SONUÇ

Bir ülkede ekonomik kalkınmanın gerçekleşmesi ve sürekliliğinin sağlanması, sağlıklı işleyen bir mali sistem alt yapısıyla büyük ölçüde ilgilidir. Bu alt yapının önemli aktörleri düşünüldüğünde ilk sırada kuşkusuz, fon fazlası olanlarla fon açığı olanlar arasında köprü vazifesi gören ve bu transfere aracılık eden bankalar yer almaktadır. Bankaların bahsedilen bu özelliği sebebiyle etkin bir risk yönetimine sahip olması gerek ulusal gerekse uluslararası piyasalarda mali istikrarın sağlanması ve sürdürülmesi için kaçınılmaz bir gereklilik haline gelmiştir.

Küreselleşme neticesinde uluslararası rekabetin artması, teknolojideki inanılmaz hızdaki gelişmeler, bankacılığı çok çeşitli ürün ve hizmet sunan bir sektör haline getirmiş, bu gelişmeler de sektördeki riskleri çeşitlendirmiş ve karmaşık bir yapıya sokmuştur. İşte bu noktada risklerin yönetimini, sektörün gözetim ve denetimini yapacak organizasyonlara ihtiyaç kendiliğinden doğmuştur. 1980'li yıllardan itibaren uluslararası arenada bankaların sermaye yeterliliği ile ilgili kaygıların artmasına paralel olarak, risklerin daha sağlıklı ölçümü yönündeki gayretler ivme kazanmış, sonuçta gelişmiş ülkelerin merkez bankaları ve bankacılık denetim otoritelerinden yetkililerin oluşturduğu Basel Bankacılık Komitesi 1988 yılında riske dayalı ilk sermaye yeterlilik uzlaşısı Basel-I'i yayımlamıştır. Basel –I'in 1992 yılında tam olarak uygulamaya geçmesiyle beraber, Uzlaşıdaki eksik taraflar belirginleşmeye başlamış, nihayet Komite 1996 yılında piyasa riskini de sermaye yeterlilik rasyosuna eklemiştir. Komite, Basel I'e yönelik zamanla ortaya çıkan eleştiriler ve sektörde gerçekleşen önemli gelişmeler evresinde yeni bir uzlaşı seti oluşturmak amacıyla 1999 yılında çalışmalara başlamıştır. Basel I düzenlemesi tek tip risk ölçümüne odaklı iken, yeni düzenleme bankalara dahili risk yönetim metodolojilerine, denetimlere ve piyasa disiplinine dayalı bir yapı getirmektedir. Basel II olarak adlandırılan yeni uzlaşı seti eskisine göre daha kapsamlı risk tanımları, ölçüm yöntemleri ve risk değerleme hassasiyetine sahiptir. Basel II bankaların maruz kaldığı riskleri; kredi riski, piyasa riski ve operasyonel risk olarak üç ana gruba ayırmıştır. 2004 Temmuz ayında yayınlanan yeni uzlaşı seti G10 ülkelerinde faaliyet gösteren ve uluslararası bankacılık yapan finansal kurumlarda 2007 yılından itibaren uygulanmaya başlamıştır. Ülkemizde de Basel-II'nin getirdiği temel değişikliklerden biri karşılanmış ve Haziran 2007 itibarıyla operasyonel risk kalemi sermaye yeterliliği hesaplamalarına dahil edilmiştir.

Basel-II kapsamında 01.01.2009 tarihinden itibaren bankaların sermaye yeterliliğinin ölçümünde esas alınacak kredi riskinin derecelendirmeye dayalı olarak hesaplanması düşünülmekteydi. Ancak 2008 yılının son çeyreğinde uluslararası finansal piyasalarda yaşanan sebepleri ve etkileri derin ve belirsiz gelişmeler ışığında özellikle seküritizasyon ve likidite riski açılarından Basel-II uzlaşısında eksiklikler tespit edilmesi, bu eksikliklerin giderilmesi amacıyla ilgili dokümanlarda değişiklik çalışmalarının uluslararası düzeyde devam etmesi, Türk Ticaret Kanunu tasarısının henüz yasalaşmaması ve finans ve reel sektör temsilcilerinin Basel-II'nin uygulanma zamanlamasına ilişkin görüşlerinin de dikkate alınması neticesinde kredi riskinin derecelendirmeye dayalı olarak hesaplanmasına ilişkin uygulamanın ileri bir tarihe ertelenmesi uygun görülmüş ve yeni bir uzlaşının yayımlanacağı beklentisi hakim olmuştur.

Türk Bankacılık Sisteminde sermaye yeterliliğinin hesaplanması 1 Kasım 2006 tarihli Resmi Gazete'de yayımlanan "Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik" esas alınarak yapılmaktadır. Buna göre Basel Komite bankaların operasyonel risk için gerekli asgari sermayenin hesaplanmasında temel gösterge yaklaşımı, standart yaklaşım, alternatif standart yaklaşım ve gelişmiş ölçüm yaklaşımları olmak üzere dört yaklaşım önermektedir. Sırasıyla her bir yaklaşım bir öncekine göre daha kapsamlı ve risk duyarlılığı daha yüksek uygulamalar içermektedir.

Temel gösterge yaklaşımında, bankaların son üç yıla ait ortalama brüt gelir tutarı risk göstergesi olarak kabul edilmekte ve bu tutar Uzlaşıda belirlenen bir katsayıyla (%15'lik alfa faktörü) çarpılarak operasyonel risk için gerekli olan sermaye yükümlülüğü hesaplanmaktadır. "Standart Yaklaşım", farklı iş kolları için farklı göstergeler kullanılarak sermaye yeterliliğini hesaplamayı hedeflemektedir. Bu yaklaşımda bankacılık faaliyetleri 8 ayrı iş koluna ayrılmış olup sermaye yükümlülüğü 8 ayrı faaliyet kolu itibariyle tespit edilen son üç yıla ait brüt gelir rakamlarının her bir faaliyet kolu için belirlenmiş olan katsayılarla (% 12, 15, 18'lik beta faktörleri) çarpılması suretiyle hesaplanmaktadır. Standart yaklaşımın bir alt kolu olan " Alternatif Standart Yaklaşım" da ticari ve perakende bankacılık faaliyet kollarında üretilen faaliyet geliri yerine, bu iş kolları dahilinde kullandırılan kredi tutarının sabit bir değer (0.035) ile çarpılması neticesinde elde edilecek risk tutarı sermaye yeterliliği hesabında dikkate alınmaktadır. Gelişmiş ölçüm yaklaşımı içinde içsel ölçüm yaklaşımı ve zarar dağılımı yaklaşımı olmak üzere iki farklı model

bulunmaktadır. Bunların uygulanabilmesi ancak bankanın operasyonel kayıplarına ilişkin sıklık ve etki verilerini içeren bir içsel veritabanı oluşturabilmesi ile mümkün olabilmektedir. Her iki modelde de bankanın faaliyet kolları ve operasyonel risk faktörlerini içeren bir risk matrisine sahip olması yaklaşımın ön şartıdır. Bankaların risk matrisi için ihtiyaç duyacakları veri setinin toplanması için en az 3 yıllık bir çalışma yapılması öngörülmektedir.

Çalışmanın ilk bölümünde; genel olarak risk yönetim kavramı, Basel-I ve Basel-II düzenlemeleri, yasal çerçeve, operasyonel risk yönetiminin temel yönleri, risk toleransı, operasyonel risk yönetiminin aktörleri, risk değerlendirme araçları, anahtar risk göstergeleri, anahtar performans göstergeleri, operasyonel kayıp veri tabanının oluşturulması gibi operasyonel risk yönetiminin unsurları ve araçları hakkında bilgi verildikten sonra ikinci bölümde COSO'nun kurumsal risk yönetimi modeli ve operasyonel riskin dört ana faktörünü oluşturan "insan", "sistem", "süreç" ve "dışsal faktörler" için önerilen operasyonel risk yönetimi uygulamaları anlatılmıştır.

Çalışmanın üçüncü bölümünde uygulama kısmında sayısallaştırılması diğer riskler gibi kolay olmayan operasyonel risklerle ilgili olarak sektörün ve sektördeki bankaların operasyonel risk yönetimi konusunda ne seviyede olduklarını belirlemeye yönelik olarak olgunluk modeli ve analitik hiyerarşi süreci yöntemi kullanılarak bankalar için ORYOS endeksinin belirlenmesine yönelik kurulan model açıklanmıştır.

Çalışmanın son bölümünde ampirik çalışmanın bulguları anlatılmış ve yapılan anket çalışmasının sonuçları istatistiki analize tabi tutulmuştur. Anket operasyonel riskin kaynağını oluşturan "İNSAN", "SİSTEM", "SÜREÇ" ve "DIŞSAL ETKENLER" olmak üzere dört ana bölümden oluşmuştur. Her bir bölüm kendi içinde çeşitli sayıdaki alt faktörlerden oluşan değerlendirme cümlelerinden kurulmuştur. Bu cümlelerin birbirlerine göre göreli önem dereceleri de analitik hiyerarşi süreci yöntemiyle belirlenmiştir. Ankette, bankalardan dört ana bölümden (insan, sistem, süreç, dışsal faktörler)oluşan toplam 33 adet cümleyi değerlendirmesi istenmiştir. Dört ana faktör içinde yer alan 33 adet değerlendirme cümlesinin her birinin altında olgunluk seviyesi sıfır (yok, varolmayan) ile beş (en iyi uygulama, optimize edilmiş) arasında değişen 6 farklı seviyede cümle yer almıştır. Bankalardan istenen 33 adet değerlendirme cümlesinin her biri için altlarında yer alan 6

farklı seviyedeki cümlelerden kendi durumlarını en iyi yansıtan cümleyi seçmek olmuştur ki seçilen cümlelerin her biri bir olgunluk seviyesine karşılık gelmektedir.

Anket TCMB hariç sektörde faaliyet gösteren tüm bankalara gönderilmiştir. Toplam 49 bankanın 42'si ankete cevap vermiştir. Sahiplik ve faaliyet açısından ankete katılan banka grupları incelendiğinde; katılım bankaları ile kamuya ait kalkınma ve yatırım bankalarının tamamı, kamu mevduat bankalarının %75'i, yerli özel sermayeli mevduat bankalarının %82'si, yabancı mevduat bankalarının %88'i, yerli özel kalkınma ve yatırım bankaları %80'i ve yabancı sermayeli kalkınma ve yatırım bankalarının %75'i ankete katılmışlardır. Ankete katılım yüzdesi toplam banka sayısı açısından %86 olup ankete katılan bankaların aktif toplamları sektörün aktif toplamının %99'una isabet etmektedir ki bu oran katılımın fevkalade yüksek olduğunu göstermektedir.

Ankete verilen cevaplardan her banka için dört ana faktör altında yer alan 33 adet alt faktör için 0 ile 5 arasında olgunluk seviye puanı tespit edilmiştir. Bu puanlar AHS yöntemiyle belirlenmiş her bir ana faktör altındaki alt faktörlerin göreli önem dereceleriyle ağırlıklandırılmıştır. Her bir ana faktör altındaki alt faktör grupları için hesaplanan puanlar toplanarak ilgili ana faktör grubunun AHS ile ağırlıklandırılmış olgunluk seviyesi belirlenmiştir. Yani sonuçta bir bankanın dört ana faktör için hesaplanmış dört tane olgunluk seviyesi puanına ulaşılmıştır. Bu dört ana faktörün aritmetik ortalaması alınarak bankanın AHS ile ağırlıklandırılmış genel olgunluk seviyesi puanına ulaşılmıştır. Sonuçta hem bankacılık sektörünün, hem de sahiplik ve faaliyet açısından banka grupları için 14 farklı ***"ORYOS Endeksi"*** oluşturulmuştur.

Çeşitli grafiklerle bankaların ORYOS endeksleri sahiplik ve faaliyet açısından gruplanan banka türleri ve tüm bankacılık sektörü ortalaması ile karşılaştırılmış ve aralarındaki farklar görsel olarak analiz edilmeye çalışılmıştır.

Anket sonuçlarının istatistiki açıdan analiz edilerek bir dizi test ile kurulan hipotezler incelenmiştir. Öncelikle anketin (ölçeğin) güvenilirliği Alfa Yöntemi (Cronbach Alfa Katsayısı) ile değerlendirilmiştir. Bu değerlendirme anketin dört ana faktörü ve tümü için ayrı ayrı yapılmıştır. "İnsan" faktörüne ilişkin likert ölçekli değerlendirme cümleleri için yapılan güvenilirlik analizinde alfa katsayısı 0.969, "sistem" faktörü için 0.982, "süreç"

faktörü için 0.981, “dışsal etkenler” faktörü için 0.980 ve nihayet bankaların operasyonel risk yönetimi olgunluk seviyesini ölçmek için hazırlanmış ölçeğin tümü için alfa katsayısı 0.994 olarak hesaplanmıştır ki bu da operasyonel risk yönetimi kriterlerine ilişkin hazırlanmış likert ölçekli ifadelerin çok güvenilir olduğunu göstermektedir.

Korelasyon analizi ile bankalar için hesaplanan ORYOS endeksi ile diğer bazı değişkenler arasındaki doğrusal veya eğrisel ilişkinin derecesi araştırılmıştır. Analiz sonuçlarına göre ORYOS endeksi ile bankaların personelinin eğitim düzeyi arasında %39 gibi doğrusal ama nispeten zayıf bir ilişki olduğu görülmüştür. Bankaların yabancı sermaye oranı ile ORYOS endeksi arasındaki doğrusal ilişki derecesi incelendiğinde istatistiki açıdan çıkan sonuçların anlamlı olmadığı görülmüş, bu durumda değişkenler arasında eğrisel bir ilişkinin varlığı analiz edilmiştir. %46 gibi bir oranda bu iki değişken arasında pozitif bir eğrisel ilişki olduğu görülmüştür. Sektörde faaliyet gösteren ve sektöre girdiğinden itibaren yabancı statüsünde olan bankalarla satın alma ve devir neticesinde sonradan yabancı olan bankaların ORYOS endeks puanları arasındaki ilişki araştırılmış, aralarında anlamlı ve doğrusal ya da eğrisel bir ilişki görülmemiş, bunun gözlem sayısının azlığından kaynaklandığı düşünülmüştür. Bankaların yaşı ile ORYOS endeksi karşılaştırılmış aralarında anlamlı bir doğrusal veya eğrisel ilişki görülmemiştir. Bankalardaki toplam personel sayısı ile ORYOS endeksi karşılaştırılmış ve aralarında %33 gibi nispeten zayıf, pozitif yönlü doğrusal bir ilişki olduğu görülmüştür. Bankaların şube sayısı ile ORYOS endeksi karşılaştırılmış ve aralarında %30 gibi pozitif ama çok güçlü olmayan bir ilişki görülmüştür.

Sahiplik ve faaliyet açısından gruplanan bankaların kendi grubu içerisindeki banka türleri arasında ORYOS endeksi açısından anlamlı bir fark olup olmadığı varyans analizi ile test edilmiştir. Öncelikle varyans analizinin ön şartı olan varyansların homojenliğinin sağlanıp sağlanmadığı test edilmiş, varyans homojenliği sağlanan ortalamalar için varyans analizi yapılmıştır. Faaliyet açısından gruplanan bankaların (mevduat, kalkınma&yatırım, katılım) ORYOS endeksleri arasında anlamlı bir fark olup olmadığı araştırılmış, %95 güven aralığında böyle bir fark olmadığı görülmüştür. Yani bu gruptaki banka türlerinden biri diğerine göre operasyonel risklerini daha iyi veya daha kötü yönetiyor diye bir şey söylenememiştir. Varyans analizi aynı şekilde operasyonel riskin dört ana faktörü için faaliyet türlerine göre ayrılan gruplara yönelik olarak yapılmıştır. Yani örneğin insan faktörü

için bankaların faaliyet türlerine göre ORYOS endeksleri arasında anlamlı bir farklılık olup olmadığı araştırılmıştır. Aynı şekilde “sistem”, “süreç” ve “dışsal etkenler” faktörleri için de ayrı ayrı bankaların faaliyet türlerine göre ORYOS endeksleri arasında anlamlı bir farklılık olup olmadığı araştırılmıştır. Hepsi için çıkan ortak sonuç; bu dört faktör için bankaların faaliyet türlerine göre ORYOS endeksleri arasında anlamlı bir fark olmadığıdır. Yani örneğin mevduat bankalarında “insan” faktörüne ilişkin ORYOS endeksi, katılım bankalarının “insan” faktörüne ilişkin ORYOS endeksine göre anlamlı bir farka sahip değildir. Varyans analizleri sahiplik açısından banka türleri (kamu, yabancı, yerli özel) için de yapılmıştır. Burada incelenen hipotez sahiplik açısından gruplanan bankaların ORYOS endeksleri arasında anlamlı bir fark olup olmadığının araştırılmasıdır. Varyans analizi aynı şekilde operasyonel riskin dört ana faktörü için sahiplik türlerine göre ayrılan gruplara yönelik olarak yapılmıştır. Sahiplik açısından banka türleri için kurulan hipotezlerde çıkan ortak sonuç; bankaların ORYOS endeksleri (genel) ve dört ana faktör için hesaplanan ORYOS endeksleri (insan, sistem, süreç, dışsal etkenler) arasında istatistiksel açıdan anlamlı bir fark olmadığıdır.

Kümeleme analizi ile bankaların hesaplanan ORYOS endekslerine göre kendi aralarında anlamlı kaç farklı gruba ayrıldığı ve her bir üyenin hangi grup içerisinde yer aldığının tespit edilmesi amaçlanmıştır. Analiz sonucunda bankalar üç farklı kümede toplanmıştır. Her bir küme içerisinde yer alan bankalar sahiplik ve faaliyet açısından incelendiğinde; her bir kümede toplanan bankaların sahiplik ve faaliyet açısından belli türleri özellikle kapsamadığı görülmüştür. Yani ORYOS endeksine göre en yüksek puan alan bankalar içerisinde yerli bankalar olduğu gibi yabancı bankalar da bulunmaktadır. Yine benzer şekilde ORYOS endeks puanlarına göre bir alt seviyedeki kümede yer alan bankalar arasında da sahiplik açısında kamu, yabancı ve yerli özel olarak sınıflandırılan bankalar olduğu gibi faaliyet açısından da bu grupta mevduat, kalkınma&yatırım ve katılım bankaları yer almıştır. Dolayısıyla kümeleme analizinde elde edilen sonuçların, varyans analizinde elde edilen sonuçları doğruladığı görülmektedir.

Böylelikle ölçülmesi ve sayısallaştırılması en zor risk türü olan operasyonel riskin bankalarda yönetim seviyesini bulmak için olgunluk modeli kullanılarak bankalar için ORYOS endeksi yaratılmıştır. Bu endeks ile bankalar hem münferit olarak kendi risk yönetim seviyelerini görecekler hem de hesaplanan 14 farklı ORYOS endeksi ile

sektördeki yerlerini diğer banka grupları ile karşılaştırmalı olarak analiz edebileceklerdir. Ayrıca bulunan bu endekse bağlı olarak belirlenecek ORYOS sermaye yükümlülük çarpanı ile de bankanın operasyonel risk yönetim seviyesi sermaye yeterliliği standart oranının hesaplanmasında bir değişken olarak kullanılabilecektir. ORYOS çarpanını düzenleyici otoritenin önerdiği temel gösterge yaklaşımı, standart yaklaşım ve alternatif standart yaklaşım için kullanmak pratikte hiç de zor değildir. Kaldı ki bankalar her iki yılda bir BDDK'nın düzenlemesiyle bağımsız denetim firmaları kanalıyla bilgi sistemleri denetimine, her yıl da uygulama kontrolleri denetimine tabi olmaktadırlar. Yapılan bu denetimler neticesinde varılan noktada şu an itibariyle bankalardan durumlarını düzeltmeleri için aksiyon almaları istenmekte ama sonuçlar kamuoyu ile paylaşılmamaktadır.

COBIT ve uygulama kontrolleri denetimlerinde bakılan noktalar, incelenen hususlar aslında operasyonel risk yönetim seviyesini belirlemeye yönelik işlemlerin özünü oluşturmaktadır. Her ne kadar denetimin adı bilgi sistemleri denetimi olsa da bakılan noktalar operasyonel riski oluşturan dört ana faktörü -"insan", "sistem", "süreç" "dışsal faktörler"- tamamen içermektedir. Bu itibarla düzenleyici otoritenin uygulanmakta olan bilgi sistemleri denetiminin kapsamını biraz daha genişletip bankaların operasyonel risk yönetim seviyelerini periyodik olarak bağımsız denetim veya Kurumun kendi denetim elemanları aracılığıyla, çalışmada önerilen ORYOS endeksine göre ölçüp puanlamaları ve sektöre yönelik hesaplanan 14 farklı ORYOS endeksinin periyodik denetimler neticesinde kurumsal şeffaflığın sağlanması amacıyla düzenleyici otorite tarafından kamuoyu ile paylaşılması önerilmektedir.

Ayrıca ORYOS endeksine bağlı olarak düzenleyici otorite tarafından belirlenecek olan ORYOS sermaye yükümlülük çarpanı, sermaye yeterlilik standart oranının hesaplanmasında kurumların mevcut operasyonel risk yönetim seviyelerini dikkate alan bir düzeltici değişken olarak kullanılarak, operasyonel risk için sermaye gereksinimi hesaplamasında daha gerçekçi bir ölçüm metodolojisine ulaşılacağı düşünülmektedir.

EK

BANKALARDA OPERASYONEL RİSK YÖNETİMİ OLGUNLUK SEVİYESİNİN BELİRLENMESİNE YÖNELİK ANKET

A) İNSAN

İK01) İnsan Kaynakları Yönetim Metodolojisi

İnsan kaynakları yönetim metodolojinize ilişkin Kurumunuzun durumunu değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumun insan kaynakları yönetimine ilişkin özel bir politikası bulunmamaktadır.

☐ Yönetim insan kaynaklarına yönelik belirli bir politikanın oluşturulması gerektiğinin farkında olmasına karşın mevcut uygulama klasik personel işlemleri şeklinde yürütülmektedir.

☐ Personel yönetimi ve alımı esas itibariyle proje bazlı gerçekleşmekte olup eğitimler ihtiyaç duyulduğunda sağlanmaktadır.

☐ Kurumun insan kaynakları yönetimine ilişkin stratejik bir yaklaşımı ve süreci düzenleyen yazılı bir politikası mevcut olup, yeni personel alımı, personelin eğitimi, kurum içi rotasyonu gibi hususlar bu politika çerçevesinde yürütülmektedir.

☐ Kurumun insan kaynakları yönetiminden konuyla ilgili alanda yetişmiş, eğitim almış bilgi ve tecrübe sahibi kişiler sorumlu olup insan kaynakları politikası değişimlere açık, personelin işten ayrılış hızı veya büyümesi gibi tanımlar vasıtasıyla ortaya çakabilecek sorunların önceden tespitine dönük göstergelerle proaktif olarak izlenmekte ve gözden geçirilmektedir.

☐ İnsan kaynakları yönetim planı değişen iş koşullarına göre güncellenmekte olup mevcut kaynakların en verimli şekilde kullanılmasını sağlamaktadır. İnsan kaynakları politikası, kurumun stratejik planıyla uyumlu olup, ücretlendirme, sektörel tartışmalara katılım, bilgi transferi, sürekli eğitim gibi sektördeki en iyi uygulamalar ile de uyumludur.

İK02)Eğitim Politikası

Kurumunuzun personele sağladığı eğitim faaliyetlerine ilişkin size en uygun seçeneği (X) ile işaretleyiniz.

☐ Personele yönelik olarak bir eğitim programı düzenlenmesi konusunda kurumda bir farkındalık oluşmamıştır.

☐ Kurum, personel için tasarlanmış eğitim ve uygulama programlarının oluşturulması gerektiğinin farkında olmasına karşın süreci düzenleyen standart bir prosedür olmadığından genellikle personel ihtiyaç duyduğu eğitime kendisi karar vermekte ve katılmaktadır.

☐ Kurum, eğitim ve uygulama programları ve bunlarla ilişkili diğer süreçlerin oluşturulması gerektiğinin farkındadır. Eğitim ihtiyaçları performans değerlendirmesinde ve planlanmasında yer almaya başlamıştır. Eğitim ve uygulamalara dönük süreçlerin işlemesi önemli ölçüde kişisel gayretlere bağlıdır.

☐ Eğitim ve uygulamalara dönük tanımlanmış bir süreç mevcut olup, çalışanlar ve yöneticiler eğitim ihtiyaçlarını tespit edip bir program dahilinde ilgili birimlere bildirebilmekte, ihtiyaçlar ve talepler bütçe ile planlanmaktadır.

☐ Yönetim, düzenlenen eğitim ve uygulama programlarını desteklemekte, kariyer planlamasının önemli birer parçası olduğunu kabul etmekte ve sürekli olarak geliştirerek izlemektedir.

☐ Kurumun sektördeki en iyi uygulamaları referans alan, üst yönetimin tam desteğini almış, kariyer planlamasının önemli birer parçasını oluşturan, çalışanların performansını ve motivasyonunu yükselten, gerektiğinde kurum dışından uzmanlar tarafından da danışmanlık alınarak sürekli olarak iyileştirmeye açık bir eğitim politikası mevcut olup kesintisiz uygulanmaktadır.

İK03)Suiistimallerin Önlenmesi ve Etik İlkelere Uyum

Kurumunuzda suiistimallerin önlenmesi ve personelin etik ilkelere uyumuna ilişkin mevcut durumunuzu değerlendirerek durumunuza en uygun seçeneği (X) ile işaretleyiniz

☐ Kurumda suiistimallerin önlenmesi ve personelin etik ilkelere uyumunun gerekliliği konusunda bir farkındalık oluşmamıştır.

☐ Etik ilkeler setinin çalışanlara duyurulmasının gerekli olmadığı düşünülmekte, suiistimallere dönük yaklaşım ise önleyici olmaktan ziyade tespit edici niteliktedir.

☐ Etik değerler seti oluşturulmuş olmasına karşın, çalışanların bu unsurlara ne derecede uygun davrandığı izlenmemektedir. Disiplin uygulamaları da yeknesak olmadığı gibi suiistimallerin önceden tespitine dönük tutarlı işleyen bir politika yoktur. Ayrıca, personelin şikayet, uyarı vb. mesajlarını ilgili birimlere iletmesi düzensiz bir şekilde gerçekleşmektedir.

☐ Tüm çalışanların uyması gereken etik değerler ve disipline dönük konular dokümante edilmiş, her bir personele basılı olarak teslim edilmiş olup, suiistimallerin önlemesine dönük hesap kontrolleri zaman zaman gerçekleştirilmektedir.

☐ Kurumun etik prensipleri kamuyla paylaşılmış olup kamusal denetime tabi olduğunu vurgulamaktadır. Ayrıca, etkin işleyen bir iç kontrol sistemi tesis edilerek olası suiistimaller önceden tespit edilmeye çalışılmaktadır. Ortaya çıkan suiistimallere ilişkin kayıtlar tutulmakta ve çeşitli ölçüler kullanılarak risk azaltıcı analizler yapılmaktadır.

☐ Kurumda suiistimallerin önlenmesi ve tespit edilmesine yönelik olarak oluşturulmuş sistemsel alt yapı ile işlemler özel programlar vasıtasıyla izlenmekte, sıra dışı işlemler anında üst yönetime ve iç sistem birimlerine raporlanmakta ve bu konuda uluslararası firmalardan eğitim ve danışmanlık alınmaktadır.

İK04)Görev Tanımları

Kurumunuz personeline ait görev tanımlarına ilişkin durumunuza en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda çalışan her bir personelin görev, yetki ve sorumluluklarının yazılı bir şekilde belirlenerek bir portal veya bir intranet üzerinden takip edilmesi gerektiğine dair bir farkındalık oluşmamıştır.

☐ Kurumda çalışanların görevler ayrılığı prensibine uygun olarak görev tanımlarının hazırlanması konusunda bir fikir yönetimce kabul görmüş ve bir kısım personelin görev tanımları yazılı olarak oluşturulmuştur.

☐ Görev tanımları tüm birimler tarafından oluşturulmaya başlanmış olmasına karşın, belli ve standart prosedürler olmadığından oluşturulan görev tanımları biçim ve içerik yönünden farklılıklar göstermekte ve güncelliği gecikmeli olarak gerçekleştirilmektedir.

☐ Her bir personelin rol ve sorumluluklarını belirleyen görev tanımları görev ayrılığı ilkesine göre dokümante edilmiş, yetkileri sisteme tanımlanmıştır. Görev tanımlarında ve organizasyonel yapıda zamanla meydana gelen gelişmelerin dokümantasyona yansıması veya sistemsel olarak sahip olunan yetkilerin geçerliliği incelenmemektedir.

☐ Personele ait görev tanımları dokümantasyon izleme programları ile sistem üzerinde takip edilmekte, güncellenme, arşivleme gibi hususlar dokümantasyon programları aracılığıyla yapılmaktadır.

☐ Personelin görev tanımlarının kurum içerisinde izlenmesi, güncellenmesi, arşivlenmesi gibi yönetilmesine ilişkin hususlar sektördeki en iyi uygulamalar baz alınarak sistem üzerinde programlar vasıtasıyla yerine getirilmektedir. Kurumun uygulaması sektöre referans teşkil eder niteliktedir.

İK05)Personel İşe Alım- İşten Ayrılış Süreci

Kurumunuzun personel işe alım, işten ayrılış sürecini düzenleyen politikalarını değerlendirerek mevcut durumunuzu en iyi yansıtan seçeneği (X) ile işaretleyiniz.

☐ Kuruma yeni personel alımını/ayrılışını düzenleyen her hangi bir doküman yoktur. Ayrıca işe alım sürecinin insan kaynağının değerini belirleyen önemli süreçlerden biri olduğu düşünülmemektedir.

☐ Personel alımına/ayrılışına ilişkin sürecin prosedüre edilmesi gerekliliği kabul edilmekle beraber, şu an itibariyle bu süreç kurumun bir kaç personelinin kendi tecrübelerine bağlı olarak yürütülmektedir.

☐ Kurum içindeki bir kaç tecrübeli çalışan tarafından yürütülen personel alım/işten ayrılış süreci bu kişiler tarafından yazılı olarak prosedüre edilmeye başlanmıştır. İşe alım sürecinde düzenli olmamakla beraber bazı birim ve unvandaki adaylar için kişilik testleri ve özgeçmiş doğrulaması yapılmaktadır.

☐ İşe alım/işten ayrılış süreci baştan sona prosedüre edilmiş olup, bu süreçte yapılması gereken testler (psikometrik ve yetenek testleri), öz geçmiş doğrulması gibi işlemler yapılmakta fakat sürecin birebir prosedürlere göre işlediği denetlenmemektedir. Ayrıca insan kaynakları biriminde çalışan personele konuyla ilgili eğitimler, çalışanların talepleri doğrultusunda verilmektedir.

☐ İnsan kaynakları yönetim süreci en kapsamlı ve detaylı şekilde prosedüre edilmiş, etkinliği ve işleyişi belirli metriklerle yönetim tarafından izlenmekte ve sürecin sürekli iyileştirme çalışmaları devam etmektedir.

☐ Kurumun insan kaynakları yönetim süreci, bu alanda uluslararası hizmet veren kuruluşlardan danışmanlık alınarak ve sektördeki en iyi uygulamalar referans alınarak oluşturulmuş programlarla ve projelerle yürütülmekte olup sektördeki diğer kuruluşlara örnek teşkil edecek niteliktedir.

İK06)Performans Yönetimi

Kurumunuzun performans ölçüm ve değerlendirme sistemini değerlendirerek mevcut durumunuzu en iyi yansıtan seçeneği (X) ile işaretleyiniz.

☐ Personelin belli periyotlarda performanslarının ölçülmesi ve değerlendirilmesine ilişkin Kurumun belli bir politikası yoktur.

☐ Kurumda çalışanların belli periyotlarda performanslarının ölçülmesi ve değerlendirilmesinin gerekliliği konusunda bir farkındalık oluşmuş, bu konuda bazı çalışmalara başlanmıştır.

☐ Kurumun bir çok biriminde benzer ölçütlerden hareketle önceden belirlenmiş hedefler doğrultusunda çalışanların performansı ölçülmekte olup performans

yönetimine ilişkin standart prosedürler ve eğitimler olmadığından performans değerlendirmesi yöneticilerin ve ilgililerin kişisel tecrübelerine göre yapılmaktadır.

☐ Kurumda üst ve orta düzey yöneticilerle diğer personel için oluşturulmuş performans hedefleri ve metrikleri mevcut olup bunlar yazılı olarak prosedüre edilmiş ve uygulanmasına karşın ücretlendirme ve terfi politikasında performans sistemi belirleyici rol oynamamaktadır.

☐ Kurumun onayladığı resmi bir performans yönetim sistemi mevcut olup, söz konusu süreç sistem üzerinde kurulmuş programlarla işletilmekte ve personelin performansı yöneticiler tarafından bu programlar vasıtasıyla istenildiği zaman otomatik olarak ölçülüp raporlanabilmektedir. Sürecin işleyiş etkinliği yönetimce izlenmekte ve iyileştirmeye dönük çalışmalar yapılmaktadır.

☐ Süreç iyileştirme kapsamında danışmanlık hizmeti alınmakta, performans ölçüm sistemi diğer insan kaynakları süreçleriyle entegre bir şekilde çalışmakta, ücret ve terfi politikasının önemli bir bileşenini oluşturmakta olup sektördeki en iyi uygulamalara referans gösterilmektedir.

B) SİSTEM

Sİ01)Bilgi Teknolojileri Risk Tanımlama ve Değerlendirme

Kurumunuzun bilgi teknolojileri (BT) risk yönetimine ilişkin risk tanımlama ve değerlendirme süreçlerini değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurum bilgi teknolojilerine ilişkin risklerin neler olduğu ve bunların dokümantasyonu konusunda bir çalışma yapmamıştır.

☐ Bilgi teknolojileri ile ilgili riskler her zaman ön planda değerlendirilmemekte, risk değerlendirmesi informal bir şekilde gerçekleştirilmektedir.

☐ Risk değerlendirmesi genellikle önemli varlık ve projeler kapsamında ya da çeşitli problemler ortaya çıktıktan sonra ilgili yöneticinin inisiyatifi doğrultusunda uygulanmakta olup gerekli aksiyonlar risklerin tespit edilmesinden sonra alınmaktadır.

☐ Kurumun bilgi teknolojileri kaynaklı tüm varlık ve uygulamalarını kapsayacak şekilde hazırlanmış olan risk yönetim politikası risk değerlendirilmesinin ne zaman ve nasıl yapılacağını tanımlamaktadır.

☐ Kurumda bilgi teknolojileri kaynaklı tüm riskler belirlenmiş, dokümante edilmiş ve bunların sahiplik sorumluluk atamaları yapılmış olup, bilgi teknolojileri yönetimi risklerin değerlendirilmesi, risk/getiri oranlarının belirlenmesi için standart ölçütler belirleyerek risk yönetimine ilişkin bir veritabanı oluşturulmuştur.

☐ Bilgi teknolojileri risk yönetimi sektördeki en iyi uygulamalar dikkate alınarak tüm kurum seviyesinde uygulanmaktadır. Kurumda risk yönetiminde kullanılan verilerin derlenmesi, analiz edilmesi ve raporlanması konusunda kurum dışından konunun uzmanlarından danışmanlık alınarak otomatik yazılımlarla yapılmakta ve risk değerlendirmesi yapılmadan herhangi bir yatırım veya projeye girişilmemektedir.

Sİ02)Bilgi Teknolojileri Alt Yapısının Yenileme ve Bakımı

Kurumunuzun bilgi teknolojilerine (BT) ilişkin alt yapısını, onun yenilenmesini ve bakımını en fazla yansıtan seçeneği (X) ile işaretleyerek belirtiniz.

☐ Bilgi teknolojilerine ilişkin alt yapı yönetiminin önemi yeterince bilinmemekte olup yenilenmesi ve bakımına ilişkin bir farkındalık oluşmamıştır.

☐ Kurum içinde bilgi teknolojilerinin önemli olduğuna ilişkin bir farkındalık mevcut olsa da gerçekleştirilen bakım ve değişiklikler kapsamlı bir planla takip edilmemekte ve sadece kısa dönemli ihtiyaçları karşılamaktadır.

☐ Bilgi teknolojileri alt yapısının yenilenmesi ve bakımına ilişkin tutarlı fakat çok kapsamlı olmayan bir politika mevcut olmakla beraber, bilgi teknolojileri alt yapısının yenilenmesi ve bakımı, önceden tanımlanmış bir stratejiye göre yapılmayıp mevcut ihtiyaçları göz ardı etmektedir.

☐ Kurumun bilgi teknolojileri alt yapısının yenilenmesi ve bakımına ilişkin; açıkça ve net şekilde tanımlanmış, planlı ve koordineli bir şekilde yürütülen ve iş stratejileriyle uyumlu bir süreç mevcuttur.

☐ Bilgi teknolojileri alt yapısının yenilenmesi ve bakım süreci mevcut uygulamalar için iyi düzenlenmiş olup, işlerliği ve tutarlılığı izlenmekte ve daha ileri seviyelere ve etkinliğe ulaşabilmesi için çalışmalar yapılmaktadır.

☐ Bilgi teknolojileri altyapısına ilişkin performans seviyeleri ileri teknoloji/yazılım kullanılarak, danışmanlık alınarak ve tüm süreçlerde tam otomasyon sağlanarak optimum şekilde ölçülerek maliyetler azaltılmaktadır.

Sİ03)Uygulamaların Test Edilmesi

Kurumunuzda geliştirilen bilgi teknolojileri uygulamalarına ilişkin test ortamınızı değerlendirerek size en uygun seçeneği (X) ile işaretleyerek belirtiniz.

☐ Programların test edilmesi gerektiğine ilişkin bir farkındalık olmayıp, programlar test edilmeden gerçek ortama aktarılmaktadır.

☐ Program testleri için ayrı bir ortam bulunmamakta, testler gerçek ortamda gerçekleştirilmektedir.

☐ Program testlerinden bazıları gerçek ortamdan ayrı bir test ortamında yapılmakta bazıları da gerçek ortam içerisinde test edilmektedir.

☐ Uygulamaların geliştirildiği test ortamı ve gerçek ortam birbirinden tamamen ayrılmıştır.

☐ Uygulamaların geliştirildiği test ortamı için sorumluluklar ve yapılacak kontroller tanımlanmış, testlerde ileri teknoloji kullanımına geçilmiştir.

☐ Uygulama geliştirme platformları ve diğer yönetim araçları için kurum, teknolojik çözümler içeren en ileri ve en iyi uygulamaları kullanmaktadır.

Sİ04)Bilgi Teknolojileri Performans ve Kapasite Yönetimi

Kurumunuzun bilgi teknolojileri kaynaklı performans ve kapasite yönetimi seviyesini aşağıdaki en uygun seçeneği (X) ile işaretleyerek belirtiniz.

☐ Kurumsal olarak bilgi teknolojileri kapasitesini planlamaya dönük herhangi bir plan, proje mevcut olmayıp, yönetim kritik iş süreçlerinin yüksek seviyede bilgi teknolojileri performansına ihtiyaç duyabileceği veya biriken iş ihtiyaçlarının bilgi teknolojileri kapasitesini aşabileceği konusunda yeterince değerlendirme yapmamaktadır.

☐ Yöneticiler bilgi teknolojileri performansı ve kapasitesine ilişkin belirli bir planlamanın oluşturulması gerektiğinin az çok farkında olsalar da ortaya çıkan sorunlara karşı geçici çözümler üretilmekte, geleceğe yönelik bir planlama yapılmamakta ve önlemler genellikle olaylar geliştikten sonra alınmaktadır.

☐ Performans ve kapasite ihtiyaçları ve ölçümleri ile planlamaya ilişkin problemler, müşteri ve kurum içi birimlerden ziyade genel olarak proje ve teknik destek ekiplerindeki konunun uzmanı anahtar kişilerin kişisel bilgisine göre bilgi teknolojileri biriminin ihtiyaçları göz önüne alınarak belirlenmektedir.

☐ Performans ve kapasiteyi ölçmeye yönelik olarak hizmet seviye gereksinimleri, metrikler ve performans istatistikleri raporlanmaktadır.

☐ Bilgi teknolojileri uygulamalarına ilişkin performans ve kapasite istatistikleri iş süreçleri içerisinde belirlenmiş otomatik program ve metriklerle ölçülüp raporlanmakta böylece kullanıcılar ve müşterilerin bilgi teknolojileri hizmet seviyelerini takip etmeleri ve sağlanan hizmetin yeterliliğini değerlendirmeleri sağlanmaktadır.

☐ Performans ve kapasiteyi ölçen metrikler tüm kritik iş süreçlerinde “anahtar performans göstergeleri” olarak kullanılmak ve geleceğe yönelik planlar yapmak üzere geliştirilmiş olup optimum kapasiteye minimum maliyetle ulaşılabilmesine imkan sağlamaktadır.

Sİ05)Değişiklik Yönetimi

Kurumun sahip olduğu uygulamalar, programlar ve sistemler üzerinde yapılan değişikliklerin yönetimine ilişkin aşağıdaki en uygun seçeneği (X) ile işaretleyiniz.

☐ Değişiklik yönetimine ilişkin tanımlanmış bir süreç olmadığından değişiklikler hemen hemen kontrolsüz olarak yapılmaktadır.

☐ Değişiklik yönetimine ilişkin sürecin kontrol edilmesi gerekliliği konusunda kayda değer bir dokümantasyon yoktur.

☐ Yapılan değişikliklerin çoğu informal bir çerçevede gerçekleştirilmekle birlikte söz konusu süreç bütünüyle tasarlanmadığından hata yapmaya elverişlidir.

☐ Sınıflandırmayı, önceliklendirmeyi, acil durumları, versiyonlamayı, yetkilendirmeyi içeren formal bir değişiklik yönetim süreci mevcut olmakla birlikte bu sürece uyum henüz tam gerçekleşememiş ve hatalar ve yetkisiz değişiklikler nadiren de olsa yaşanabilmektedir.

☐ Değişiklik yönetim süreci oldukça gelişmiş bir yapıda olup değişiklikler işleme alınmadan önce bir onay mekanizmasından geçirilmekte, etki analizine tabi tutulmakta ve gerçekleştirilen güncellemeler izlenmektedir.

☐ Değişiklik yönetimi, iş süreçlerinin iyileştirilmesi ile entegre olarak kurum için yeni iş fırsatları yaratmakta, kurumsal verimliliği artırmakta, en iyi uygulamalarla aynı düzeyini koruması için de düzenli olarak gözden geçirilmekte ve güncellenmektedir.

Sİ06)Bilgi Teknolojileri İş Süreklilik Planı

Kurumunuzun bilgi teknolojileri iş süreklilik planını değerlendirerek size en uygun seçeneği (X) ile işaretleyerek belirtiniz.

☐ Bilgi teknolojileri faaliyetlerinden kaynaklanan riskler, tehditler ve açıklıklar ile bilgi teknolojileri hizmetlerindeki kesintinin kurum faaliyetlerine olacak etkileri henüz belirlenmemiştir.

☐ Yönetim iş sürekliliğinin sağlanmasına ilişkin risklerin farkında olarak gerekli görevlendirmeleri genel hatlarıyla yapmış olsa da kullanıcılar sistem kaynaklı hatalar karşısında kendilerine özgü yöntemler geliştirerek işlerini devam ettirmektedirler.

☐ İş sürekliliğinin sağlanmasına yönelik tam anlamıyla dokümante edilmiş bir plan ve resmi bir görevlendirme olmamasına karşılık temel ilkeler bilinmekte ve süreç kişisel gayretlere bağlı olarak yürütülmektedir.

☐ İş sürekliliğinin planlaması ve testine ilişkin sorumluluklar dokümante halde mevcut olan iş süreklilik planında yönetim tarafından net biçimde tanımlanmış olup, plan

periyodik aralıklarla test edilmekte ve kendi girişimleriyle de olsa personel belirli eğitimlere katılmaktadır.

☐ İş sürekliliği kapsamında ihtiyaç duyulabilecek olan tüm veriler belirli ve düzgün bir yapı içinde derlenip analiz edilerek plan oluşturulmuş, sorumlular belirlenmiş ve ilgili personele gerekli eğitimler verilmiştir. Plan daha önce gerçekleştirilen testlerin sonuçlarına ve geliştirilen yeni uygulamalara göre gözden geçirilmektedir.

☐ Bilgi teknolojileri iş sürekliği planı aynı zamanda kurumsal faaliyetlerin sürekliliğine ilişkin geliştirilen planlar ile entegre bir şekilde geliştirilmiş olup, plan en kapsamlı şekilde periyodik olarak tamamen test edilmekte, sonuçlar planın güncellenmesinde girdi olarak kullanılmaktadır. Söz konusu plan sektördeki en iyi uygulamalar ve kabul görmüş standartlar düzeyinde hazırlanmıştır.

Sİ07)Bilgi Güvenlik Politikası

Bilgi güvenliği kapsamında bilgi güvenlik politikasına ilişkin Kurumunuzun durumunu değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda, bilgi teknolojileri güvenliğinin sağlanmasının gerekli olduğunu konusunda bir bilinç henüz oluşmamıştır.

☐ Kurum, bilgi teknolojileri güvenliğinin sağlanmasının gerekli olduğunu düşünmekte ve bilgi teknolojileri güvenliğine ilişkin önlemler genelde olaylar geliştikten sonra alınmaktadır.

☐ Bilgi teknolojileri güvenlik politikaları geliştirilmiş olsa da bunları uygulayacak, raporlayacak araçlar ve personel tam olarak doğru yeterli ve uygun değildir.

☐ Kurumda bilgi teknolojileri güvenliği konusunda yönetim tarafından da desteklenen bilgi teknolojileri güvenlik politikası ile uyumlu bilgi teknolojileri güvenlik prosedürleri tanımlanmıştır.

☐ Bilgi teknolojileri güvenlik politikaları ve prosedürleri özel güvenlik alanları ve bilgi teknolojileri güvenliğinin sağlanmasına yönelik süreçlerin kurumsal boyutu baz alınarak hazırlanmıştır.

☐ Kurumun tüm iş süreçlerini, kullanıcılar ve müşterilerin taleplerini dikkate alarak teknolojik araç ve uygulamalar yardımıyla optimize edilmiş ve onaylanmış bir güvenlik planı bulunmaktadır. Söz konusu plan belirlenmiş olan metrikler yardımıyla ölçülmekte ve yönetim tarafından değerlendirilerek sürekli iyileştirilmesi sağlanmaktadır.

Sİ08)Bilgi Güvenlik Test ve Analizleri

Bilgi güvenliği kapsamında yapılan test ve analizlere ilişkin Kurumunuzun durumunu değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Bilgi güvenliğini sağlamaya yönelik olarak sorumlular belirlenmemiş olup güvenlik ihlalleri raporlanmamakta ve herhangi bir aksiyon alınmamaktadır.

☐ Kurumun bilgi güvenliği konusundaki sahip olduğu seviye ölçülememekte, ihlaller karşısında verilen tepkiler belirsiz olup sorumluluklar net bir biçimde belirlenememektedir.

☐ Bilgi güvenliğine ilişkin sistem tarafından bazı veriler üretilse de bu veriler herhangi bir analize tabi tutulmamakta, sorumluluğun esasen bilgi teknolojileri birimlerinde olduğu diğer birimlerin ise sorumluluk alanında yer almadığı düşünülmektedir.

☐ Bilgi güvenlik planı kapsamındaki çözümler risk analizlerine göre şekillendirilmiş olup kurumda sızma testi gibi bilgi teknolojileri güvenlik testleri yapılmaktadır. Ayrıca bilgi güvenlik birimi tarafından güvenlik eğitimleri verilmektedir.

☐ Güvenlik testlerinin nasıl yapılacağı standart olarak belirlenmiş, dokümante edilmiş, bilgi teknolojileri güvenliğine ilişkin çeşitli metrik ve hedeflerle risk ve etki analizleri düzenli ve tutarlı şekilde yapılmaktadır. Ayrıca bilgi güvenlik eğitimleri iş birimlerinin katılımıyla belirlenmiş risk profillerine cevap verebilecek şekilde kurum çapında yapılmaktadır.

☐ Sistemin maruz kalabileceği tehditler ve açıklıklara ilişkin gerekli veriler bilgi güvenlik biriminin sorumluluğunda sistemsel olarak toplanıp gerektiğinde bu konuda kurum dışından uzmanlardan da danışmanlık alınarak analiz edilmekte ve ortaya çıkan güvenlik olaylarının kök-sebep analizleri yapılarak risklerin proaktif olarak tanımlanması, sürecin sürekli iyileştirilmesi ve gerekli aksiyonların alınması için kullanılmaktadır.

C) SÜREÇ

SU01)Operasyonel Risk Yönetiminde Kurum Kültürü

Operasyonel risk yönetiminde bankanızın kurum kültürünü değerlendirerek size en uygun seçeneği (X) ile belirtiniz.

☐ Operasyonel risk yönetiminin önemi konusunda henüz bir kurum kültürü oluşmamıştır.

☐ Operasyonel risklerin önemli olduğu ve yönetilmesi gerektiği konusunda bir anlayış olmakla beraber kurumsal olarak belirlenmiş politika ve düzenlemeler henüz temel düzeydedir.

☐ Operasyonel risklerin aktif olarak yönetilmesi konusunda kurumda bir farkındalık oluşmuş, görev dağılımı yapılmış olmasına rağmen sürecin nasıl yönetileceği henüz prosedüre edilmemiştir. Birimler kabul edilebilir risk seviyelerini kendileri belirlemektedirler.

☐ Kurum çapında operasyonel risk noktaları tanımlanmış, bu risklere sorumlular atanmış, konuyla ilgili eğitimler verilmektedir. Risklerin merkezi bir yapıda değerlendirilmesine ilişkin çalışmalar prosedüre edilmiştir.

☐ Yönetim kurulu tüm operasyonel risklerle birlikte bilgi teknolojileri riskleri de dahil olmak üzere tüm birimler için risk toleransı ve risk tolerans seviyelerini belirlemiştir. Operasyonel risk yönetimine ilişkin süreç otomasyonda olup kritik faaliyet ve kontroller izlenmekte ve bu konuda ilgili personelin sertifika almaları desteklenmektedir.

☐ Üst yönetim aldığı kararlarda operasyonel, kurumsal ve bilgi teknolojileri risk yönetimini birbirinin ayrılmaz parçaları olarak değerlendirmekte, bu alanlardaki olaylar ve kontroller bilgisayar programları yardımıyla gerçek zamanlı olarak izlenmekte ve sürecin iyileştirilmesinde kullanılmaktadır.

SU02)Operasyonel Risk Kayıp Veritabanı

Bankanızın operasyonel risk kayıplarının bir veritabanında izlenmesine ilişkin uygulamalarını değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumun maruz kaldığı operasyonel risk kayıp verilerinin bir veritabanında izlenmesine ilişkin bir farkındalık oluşmamıştır.

☐ Banka, tasarımını henüz tamamlamamış olmasına rağmen karşılaştığı operasyonel risk kayıp verilerinin bir veritabanında izlenmesi gerektiğini düşünmektedir.

☐ Operasyonel kayıplara ilişkin verilerin kayıt altına alınması için bazı iş kollarında risk değerlendirmeleri gerçekleştirilmiş ve kayıp türleri belirlenmeye başlanmıştır.

☐ Temel iş kolları bazında operasyonel kayıplar sınıflandırılmış, kayıp türleri belirlenmiş, limitler tanımlanmış ve veritabanının nasıl tasarlanacağı ve yönetileceği dokümante edilmiştir.

☐ Operasyonel kayıp veri tabanı oluşturularak, iş kolları bazında sınıflandırılmış, türleri, limitleri belirlenmiş olan operasyonel kayıpların yanı sıra operasyonel kayba yol açma olasılığı olan veriler de bu veri tabanında kayıt altına alınmakta ve veritabanının işleyişi, yeterliliği izlenmektedir.

☐ Tüm iş kollarını içerir şekilde operasyonel kayıp ve olası kayıp türleri belirlenmiş, banka genelini kapsayacak şekilde veri ve bilgi aktarımının sağlanabilmesi için tüm şube ve birimleri de içeren gerekli alt yapı oluşturulmuş olup her bir iş kolundan gerekli gösterge verisi elde edilmekte ve kayıp dağılımları, skor kart, yapay sinir

ağları, senaryo analizleri, melez yaklaşımlar gibi ileri ölçüm yöntemleri kullanılarak operasyonel riskler sayısallaştırılıp ölçülebilmektedir.

SU03)Operasyonel Riskin Tanımlanması ve Değerlendirilmesi

Kurumunuzdaki süreçlere yönelik olarak operasyonel risklerin tanımlanması ve değerlendirilmesine ilişkin size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda süreçlere ilişkin operasyonel risk noktaları tespit edilmemiş ve böyle bir değerlendirmenin yapılması gerektiği konusunda bir farkındalık oluşmamıştır.

☐ Süreçlere ilişkin operasyonel risklerin belirlenmesi ve dokümante edilmesi gerektiği konusunda kurumda bir fikir birliği oluşmuş olup risklerin tespit edilmesi düşünülmektedir.

☐ Kurumdaki bazı kritik süreçlere dönük operasyonel risk tanımlamaları gerçekleştirilmiş olmasına karşın, uygulanan yöntem standart olmayıp ilgili yöneticinin inisiyatifinde olduğundan birimler arasında tam bir yeknesaklık sağlanamamıştır.

☐ Kurumun operasyonel risk değerlendirme politikası, tüm kurumu kapsayacak şekilde uygun bir metodoloji ile hazırlanmış ve dokümante edilmiş olup operasyonel risklere ilişkin öz değerlendirmeler yapılmaktadır.

☐ Kurumda hazırlanmış olan standart risk tanımlama prosedürleri çerçevesinde tüm süreçleri içerecek şekilde operasyonel riskler, anahtar risk göstergeleri ve performans göstergeleri tanımlanmakta, raporlanmakta ve izlenmektedir.

☐ Süreçlere ilişkin operasyonel risklerin tanımlanması ve değerlendirilmesi, kurumun tüm iş süreçleri ve operasyonel kayıp veri tabanı verileri ile entegre şekilde işlemekte olup sektördeki en iyi uygulamalar referans alınarak yönetim tarafından takip edilmekte ve konunun uzmanlarından danışmanlık alınmaktadır.

SU04)Operasyonel Riskin Ölçülmesi

Operasyonel riskin ölçülmesine ilişkin Kurumunuzun mevcut durumunu değerlendirerek size en uygun seçeneği (X) ile belirtiniz.

☐ Kurum operasyonel risklerle ilgili olay ve durumların kurumun performansını nasıl etkileyeceği hakkında bir görüş ve bilgiye sahip değildir.

☐ Kurumda operasyonel risk ölçümünün yapılması gerektiği konusunda bir farkındalık oluşmasına rağmen, performansı etkileyen iş koşulları ve onlarla ilgili tehditlerin neler oldukları asgari düzeyde anlaşılmıştır.

☐ Operasyonel risklerin ölçülmesine yönelik olarak yöneticiler sorumlu olduklarını hissetmekte, bu konuda birimler arasında tartışma oturumları düzenlenmekte planlı olarak bazı risk, bağımlılık ve senaryo analizleri yapılmaktadır.

☐ Kurumda operasyonel risk değerlendirmesini yapacak ekip, veri toplamayı sağlayan araçlar ve yazılımlar belirlenmiş olup gerçekleşen operasyonel kayıp olayları ve tehdit oluşturan olaylar veri tabanına kaydedilmekte ve ölçümlerde kullanılmaktadır.

☐ Risk analizlerini gerçekleştirmek üzere kullanılan yazılım ve araçlara ilişkin çeşitli prosedürler hazırlanmış olup bunlar mevcut operasyonel yazılımlarla entegre bir şekilde çalışmaktadır. Ayrıca operasyonel risklerin ne derece etkin ve verimli bir şekilde değerlendirildiği ölçülmekte ve performans hedefleriyle ve kurumun stratejik planıyla ilişkilendirilmektedir.

☐ Kurum, operasyonel risk yönetimi kapsamında verilerin toplanması, analiz edilmesi, değerlendirmesi ve gerekli aksiyonun alınması gibi aşamaları otomatik olarak işleyen yazılım ve araçlar vasıtasıyla, uzman kuruluşlardan danışmanlık ve gerekli eğitimleri alarak gerçekleştirmektedirler. Kurum operasyonel risklerini nicel ve nitel ileri ölçüm yaklaşımları ile ölçebilmektedir.

SU05)Operasyonel Riske Karşı Aksiyon Alınması

Operasyonel riske karşı aksiyon alınmasına ilişkin Kurumunuzun mevcut durumunu değerlendirerek size en uygun seçeneği (X) ile belirtiniz.

☐ Kurumda operasyonel riskler tespit edilmekle birlikte bunlara karşı alınacak aksiyonlar konusunda bir farkındalık oluşmamıştır.

☐ Kurum operasyonel riskler karşısında bir aksiyon almasının gerekli olduğunu bilmekte, fakat riske karşı alınacak aksiyonlar konusunda yeterli teknik bilgi ve tecrübeye sahibi olmadığından bunun için izlediği yöntem riskten kaçınma veya riski sigortalatmanın dışına çıkamamaktadır.

☐ Kurumda operasyonel risklerin yönetilmesine ilişkin alınacak aksiyonlar konusunda bilgi birikimi mevcut olup, söz konusu süreç sistemli bir şekilde olmayıp bazı yöneticilerin kişisel bilgisi ve tecrübesi ile yürütülmektedir.

☐ Operasyonel riskler karşısında alınacak aksiyonlar konusunda izlenecek yöntem tanımlanmış olup, personelin sorumlulukları ve nasıl hareket edilmesi gerektiği hususları prosedüre edilmiştir.

☐ Operasyonel risklere karşı alınacak aksiyonlar kurum çapında çok iyi derecede anlaşılmış olup risk yönetim sürecini düzenleyen tüm faaliyetler prosedüre edilmiş ve kritik kontrol noktalarının etkinliği, genel olarak tüm risk yönetim sürecini izleme olanağı sunan yazılım ve uygulamalar vasıtasıyla ölçülebilir durumdadır.

☐ Kurum, en ileri teknolojik olanakları kullanarak olası riskleri ve fırsat noktalarını tespit etmekte ve alınacak aksiyonlara, uygulanacak kontrollere karar verirken de etkinlik ve verimliliği ön planda tutan programlar kullanmaktadır.

SU06)İç Kontrol Sistemi

Kurumunuzun iç kontrol sistemi ve iç kontrol ortamını değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda iç kontrol sisteminin bir bütün olarak tasarlanıp iç kontrol ortamının etkinliğinin gözden geçirilip değerlendirmesi gibi hususlarda tam bir farkındalık oluşmamıştır.

☐ Kurumda iç kontrol sisteminin tasarlanması ve etkinliğinin değerlendirilmesine ilişkin herhangi bir birim görevlendirilmemiş olup, iç kontrol ortamı süreç sahiplerinin kendi tecrübelerine bağlı olarak geliştirilmekte ve değerlendirilmektedir.

☐ Kurumda iç kontrol sisteminin etkinlik değerlendirmesine ilişkin çeşitli araçlar ve metodolojiler geliştirilmiş fakat yapılan değerlendirme süreç sahibinin bilgi ve tecrübesine bağlı olarak değişkenlik göstermektedir.

☐ İç kontrol sisteminin izlenmesi ve değerlendirilmesini düzenleyen politika ve prosedürler oluşturularak dokümante edilmiş olup, süreçlere ilişkin riskler, kontrol noktaları ve alınacak aksiyonlar bizzat operasyonel faaliyetleri gerçekleştiren personelin de dahil olduğu öz değerlendirme çalışmaları ile belirlenmiştir.

☐ İç kontrol sisteminin, önceden belirlenmiş yaklaşımlar çerçevesinde değerlendirilmesi için gerekli sistemsel araçlarla ortaya çıkan olumsuzluklar hızlı bir şekilde otomatik olarak tespit edilebilmekte, iç kontrol ortamının etkinliği ve izlenmesi sektördeki uygulamalarla karşılaştırılıp değerlendirilmektedir.

☐ Kurumun iç kontrol sistemi, uluslararası alanda faaliyet gösteren uzmanlardan danışmanlık alınarak sektördeki en iyi uygulamalar referans alınarak oluşturulmuş ve süreçlerin işleyişi ve iç kontrol ortamının etkinliği belirlenmiş metriklerle ve bilgisayar destekli programlarla ölçülmekte, izlenmekte ve sürekli iyileştirilmektedir.

SU07)Kurumsal Risk Yönetimi

Bankanızın kurumsal risk yönetimine ilişkin uygulamalarını değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Operasyonel faaliyetlerin ve karar alma süreçlerinin tanımlanmış bir kurumsal risk yönetimi yaklaşımı doğrultusunda işletilmesine ilişkin herhangi bir farkındalık yoktur.

☐ Bankada yürütülen faaliyetlere yönelik risk odaklı bir bakış açışı geliştirmek ve personelin risk algısını yüksek tutmak için risk yönetimine dönük bazı çalışmalar yapılmaktadır.

☐ Bankanın bazı kritik faaliyetlerine ilişkin prosedürler oluşturulmuş, risklilik seviyeleri ve limitler belirlenmiş ve ilgili personele risk yönetimine dönük eğitimler sağlanmıştır.

☐ Risk yönetimi kurumsal kültürün önemli bir parçasını oluşturmakta, karar alma süreçleri ve operasyonel faaliyetler risk odaklı bir bakış açısıyla gözden geçirilmekte ve gerekli prosedürler hazırlanmaktadır.

☐ Tüm süreçlerde risk odaklı bir yaklaşımla süreç sahipliği tesis edilmiş, süreçlerin etkin işlediğinin tespiti için çeşitli ölçütler geliştirilmiş olup bu değerlendirmeler sonrasında iyileştirme alanları tespit edilmekte ve aksiyonlar alınmaktadır.

☐ Kurumdaki tüm birimlerin yanı sıra müşteriler ve iş ortakları da kurumsal risk yönetim sisteminin bir parçası olup birbiriyle entegre vaziyette çalışarak kurumun risk yönetim sisteminin etkinlik ve işlevselliğini arttırmaktadır.

SU08)Proje Geliştirme

Kurumunuzdaki proje geliştirme sürecini değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda gerçek ortama aktarılmak istenen programlara ilişkin yükleme ve onay sürecini düzenleyen bir prosedür bulunmamaktadır.

☐ Programların gerçek ortama aktarılmasına ilişkin onay ve kabul sürecini düzenleyen formal bir süreç tesis edilmemiş olup gerçekleştirilen yüklemelerin beklenen amaçları karşılamasının gerektiği konusunda bir farkındalık oluşmuştur.

☐ Yapılacak testler ve testlere verilecek onay sürecini düzenleyen bir yaklaşım olmakla beraber bu herhangi bir metodolojiye dayanmamakta, testlerin nasıl yapılacağına tek başlarına sistem geliştirme ekibi karar vermekte, kapsamlı ve entegre testler yapılmamaktadır.

☐ Program geliştirme sürecindeki kullanıcı ve yazılımcı testleri, gerçek ortama aktarımlar, eğitimler, kabul ve onay süreçleri tanımlanmış ve belirli seviyede otomasyon içermesine rağmen standart değildir ve yetkililerin bireysel kararlarına dayanmaktadır.

☐ Uygulamaların geliştirme süreci detaylı bir şekilde düzenlenmiş, test ortamının nasıl olması gerektiği ve onay süreci belirlenmiştir. Sistem üzerinde yapılacak tüm önemli değişiklikler tanımlanmış olan bu sürece uygun gerçekleştirilmektedir. Geliştirilen uygulamaların kullanıcı isteklerini ne derecede karşıladığı standart metrikler vasıtasıyla ölçülebilir ve üst yönetim tarafından incelenebilir durumdadır.

☐ Gerçek ortama aktarılan uygulamalara ilişkin standart olarak bir değerlendirme ve gözden geçirme süreci mevcut olup, öğrenilen derslerle mevcut sürecin kalitesi

sürekli artırılmakta, yeni uygulamalar için stres testleri ve değişiklik yapılan uygulamalar için ise doğrulama testleri devamlı olarak uygulanmaktadır.

SU09)Kalite Yönetimi

Kurumunuzun kalite yönetim sistemini değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda uygulanan bir kalite yönetim süreci olmayıp, üst yönetim böyle bir sisteminin gerekli olduğunu düşünmemektedir.

☐ Üst yönetim, kalite yönetiminin gerekli olduğunun farkında olmasına karşın, kaliteye ilişkin değerlendirmelerini bilinen bir kalite yönetim standardına göre yapmamaktadır.

☐ Kurumda kalite yönetim sistemine dönük faaliyetler tanımlanarak izlenmekte ve uygulanmakta olup, tüm kurum operasyonlarını kapsamamaktadır.

☐ Yönetim tarafından tüm kuruma duyurulmuş olan kalite yönetim sisteminde bilgi işlem personelinden son kullanıcıya kadar herkesin rolü belirlenmiş, kalitenin tesis edilmesine ilişkin eğitim ve uygulama programları hazırlanmıştır.

☐ Kurumun tüm iş süreçlerinde hatta bağlı olan iş ortaklarında bile kalite yönetim sistemi uygulanmakta, sürece ilişkin kalite ölçümleri belirlenmiş olan standart metriklerle yapılmakta, sonuçlar fayda maliyet analizlerinde kullanılmaktadır. Ayrıca tüm kurum personelini kapsayacak şekilde kalite yönetimine ilişkin eğitim programları ve kalite memnuniyet anketleri sürekli olarak düzenlenmektedir.

☐ Kurumda kalite yönetim sistemin etkin bir şekilde işlemesine yönelik tanımlanmış bir gözetim sistemi mevcut olup kurumun kalite metriklerini kapsayan bilgi havuzuna aynı zamanda kurum dışından da veri temin edilmektedir. Kalite memnuniyet anketleri süreklilik kazanmış olup, iyileştirmeye dönük aksiyonların geliştirilmesinde son derece işlevseldir.

SU10)Kontrollere İlişkin Dokümantasyon

Kurumunuzdaki iç kontrol ortamı ve dokümantasyon yönetim sürecini değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda kontrollere ilişkin politika, prosedür ve standartların oluşturulması ve yazılı olarak dokümante edilmesi konusunda bir bilinç oluşmamıştır.

☐ Politika, prosedür ve standartlar, sürece ilişkin herhangi bir risk ortaya çıktıktan ve olaylar geliştikten sonra düzenlenip duyurulmaktadır.

☐ Kontrole ilişkin politika, prosedür ve standartların gerekliliği yönetim tarafından çalışanlar ile paylaşılsa da, bu tür düzenlemelerin hazırlanması ve günlük faaliyetler içersinde ne ölçüde dikkate alınacağı birim yöneticilerinin inisiyatifine bırakılmış durumdadır.

☐ Kurumda kalite yönetimi ve kontrol ortamını düzenleyen ve içinde politika, prosedür ve standartları barındıran yapısal bir dokümantasyon geliştirme süreci mevcut olup yönetim tarafından duyurulmuş ve bütün personelce de bilinmektedir.

☐ Kalite ve güvenliğe ilişkin farkındalığın artırılmasına dönük bir hedefi de içeren proaktif nitelikte bir kontrol ortamı tesis edilmiş olup bunlara ilişkin politika, prosedür ve standartlar oluşturulmuş, dokümante edilmiş ve çalışanların kullanımına sunulmuştur.

☐ Kurumun iç kontrol ortamı, vizyonu ve stratejik yönetim çerçevesi ile uyumlu olup sürekli olarak gözden geçirilmekte,güncellenmekte ve geliştirilmektedir. Kurumda kontrol ortamına ilişkin bir rehber oluşturmak amacıyla sektördeki en iyi uygulamalar gerek kurum içi gerekse de kurum dışı uzmanlardan danışmanlık alınarak takip edilmekte ve dokümantasyon belli bir kalite standardı çerçevesinde istisnasız yapılmaktadır.

SU11)Operasyonel İşlem Limitlerinin Belirlenmesi

Kurumunuzdaki operasyonel işlem limitlerinin belirlenmesi, kullanılmasına ilişkin süreci değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Operasyonel faaliyetlerin gerçekleştirilmesi sürecinde olası riskleri azaltmak için çeşitli limitlerin belirlenmesi gerektiği konusunda bir farkındalık oluşmamıştır.

☐ Kurumda iş süreçlerinin bazıları için görevler ayrılığı ilkelerine uygun işleyiş ve limit tahsislerinin oluşturulmasına dönük çalışmalar mevcuttur.

☐ Kritik iş süreçleri gözden geçirilerek görevler ayrılığı prensipleri doğrultusunda yeniden düzenlenmiş olup temel iş süreçlerinde faaliyet gösteren personelin uyması gereken limitler tahsis edilmiştir.

☐ Kurumun tüm operasyonel faaliyetleri gözden geçirilerek süreçler için işlem bazında ve/veya personel bazında operasyonel işlem limitleri tahsis edilmiş olup bunların güncellenmesi ve limitlere uyum konusunda prosedürler oluşturularak dokümante edilmiştir.

☐ Operasyonel risk yönetiminin bir parçası olarak tüm iş süreçleri için tahsis edilen limitlere uyum sistemsel olarak izlenmekte, loglanmakta ve iç sistem birimleri ile üst yönetime raporlanmaktadır.

☐ Operasyonel işlemlerin limitlere uyumu sistem üzerinde bulunan programlar vasıtasıyla otomatik olarak sağlanmakta ve limit ihlalleri sistemsel olarak

önlenmekte olup limit değişiklikleri en az iki aşamalı olarak kontrol ve onay süreçleriyle gerçekleştirilmektedir.

SU12)Problem Yönetimi

Kurumunuzdaki problem yönetimi sürecini değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda problem veya olay yönetiminin gerekliliği konusunda en ufak bir farkındalık yoktur.

☐ Süreçler hakkında bilgi sahibi anahtar personel kendi uzmanlık alanı ile ilgili problemler hakkında kayda değer bilgi sağlamasına rağmen, bilgi paylaşımının olmaması yeni problemlere sebep olduğu gibi zaman ve kaynak israfına da yol açmaktadır.

☐ Kurumda problem yönetim sisteminin gerekliliği, bu konuda ayrılan bütçe ve verilen eğitimlerle yönetim tarafından kabul edilip desteklenmektedir. Ayrıca personel arasında karşılaşılan problemlere ve çözüm yollarına ilişkin bilgi alışverişi dokümante edilmiş prosedürler ile sağlanmaktadır.

☐ Etkin bir problem yönetim sisteminin gerekliliği yönetim tarafından kabul edilip desteklenmekte olup bunun için gerekli olan insan kaynağı ve eğitim ihtiyacı için yeterli bütçe ayrılmış durumdadır.

☐ Problem yönetimi süreci; olay, değişiklik, konfigürasyon yönetimi gibi diğer süreçler ile bütünleşmiş, iş birimlerinin gereksinimlerini karşılamakta olup karşılaşılan problemlerin büyük çoğunluğu sürece ilişkin hedefler ve metriklerle tanımlanmakta, kaydedilmekte, raporlanmakta ve çözüm için adımlar atılmaktadır.

☐ Kurumdaki birçok uygulama olası problemler karşısında erken uyarı ve tespit edici araçlar ile proaktif bir yapıyla donatılmış olup, sürekli olarak izlenmekte, değerlendirilmekte ve ölçümlerle yapılan analizlerle sürekli iyileştirmeye tabi tutulmaktadır.

D) DIŞSAL FAKTÖRLER

DF01)Tedarikçi Performans Değerlendirmesi

Kurumunuzun üçüncü taraflardan (tedarikçiler) aldığı hizmetlere ilişkin performansı değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Üçüncü taraflarla ilişkilerde sorumluluklar, hesap verme, raporlama gibi hükümler sözleşmelerde yer almadığından hatta bunları düzenleyen standart bir politika ve prosedür olmadığından, alınan hizmetin kalitesi yeterince ölçülememekte ve değerlendirilememektedir.

☐ Tedarikçilerden alınan hizmetlere ilişkin düzenli ölçüm ve raporlamaların yapılabilmesi için standart sözleşme tiplerinin olması gerektiği hususunda bir farkındalık oluşmuştur.

☐ Tedarikçilerden alınan hizmetlerin kapsamını düzenleyen standart ve imzalanmış proforma sözleşmeler mevcut olup bunlarla ilişkileri düzenleyen süreç iş hedefleriyle uyumlu olmasa da riskler informal bir şekilde izlenmekte ve raporlanmaktadır.

☐ Üçüncü taraflardan alınan/alınacak hizmetler detaylı olarak düzenlenmiş hukuksal, operasyonel ve kontrol gereksinimlerini kapsayan standart sözleşmelere göre yapılmakta ve alınan hizmetlere ilişkin riskler ve bunları denetleyen sorumlular tarafından yazılı prosedürler çerçevesinde belirlenmektedir.

☐ Tedarik hizmetlerinden beklenen hedefler ve ölçüm metrikleri belirlenmiş ve iş hedefleriyle ilişkilendirilmiş olup, tedarikçilerin performansı, nitelikleri, riskleri, yetenekleri düzenli olarak kontrol edilip izlenmekte, edinilen bilgiler mevcut ve gelecekte alınacak hizmetlere girdi teşkil etmektedir.

☐ Hizmet alınan tedarikçiler ve bunlarla imzalanan sözleşmeler periyodik olarak bağımsız bir denetime tabi tutulmakta, performansları değişen koşullara ve metriklere göre ölçülmekte, yönetime raporlanmakta ve değerlendirilerek gerekli düzeltici aksiyonlar alınmaktadır.

DF02)İş Sürekliliğinin Sağlanması

Kurumunuzun acil durum ve iş sürekliliği planlamasındaki durumunu değerlendirerek aşağıdaki en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda iş sürekliliğinin sağlanması konusunda bir farkındalık oluşmamıştır.

☐ İş sürekliliği kapsamında alınabilecek önlemler sınırlı sayıda yapılan toplantılarda ele alınmış, bu kapsamdaki görev ve sorumluluk dağılımı henüz yapılmamıştır.

☐ İş sürekliliği planları, çalışanların önemli bir bölümünün işe gelemediği durumlar da göz önüne alınarak değerlendirilmiş fakat resmi bir iş süreklilik planı hazırlanmamıştır.

☐ İş sürekliliği planı yönetim kurulunca onaylanmış olsa da planın işlerliği ve yönetimine ilişkin kısıtlı kaynak ayrılmış, bu planın hedeflenen kurtarma süresi ve seviyeleriyle uyumu değerlendirilmemiştir.

☐ Tüm kritik iş süreçlerini kapsar şekilde hazırlanmış iş süreklilik planları mevcut olup söz konusu planlar en az yılda bir kez test edilmekte ve sonuçlar yönetim kademelerine raporlanmaktadır.

☐ Kurumun tüm iş süreçlerini kapsayan, çalışanların önemli bir bölümünün işe gelemediği veya tedarikçilerden alınan hizmetlerde sorunlar yaşandığı durumlarda bile faaliyetlerin devam edebilmesine dönük geliştirilmiş, tüm kaynak gereksinimlerini dikkate alan sektördeki en iyi uygulamaları referans alan, uluslararası alanda bu konuda uzmanlaşmış kuruluşlardan danışmanlık alınarak oluşturduğu bir iş süreklilik planı mevcuttur.

DF03)Acil Durum ve İş Süreklilik Planı Testleri

Kurumunuzda gerçekleştirilen acil durum ve iş süreklilik planı testlerinin kapsamını değerlendirerek aşağıdaki en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumun bir iş süreklilik planı olmakla beraber söz konusu plan test edilmemektedir.

☐ İş sürekliliği planının yılda en az bir kez test edilmesi düşünülmesine rağmen her yıl düzenli testler yapılamamakta ve kritik tedarikçilerin iş süreklilik planlarının yeterliliği de değerlendirilmemektedir.

☐ İş süreklilik yönetimi kapsamında kurumun belirlenmiş bir test programı mevcuttur. Ayrıca kritik tedarikçilerin acil durum ve iş süreklilik planlarının yeterliliği bilinmesine rağmen, iş sürekliliğine ilişkin hizmet seviye anlaşmaları yapılmamıştır.

☐ İş sürekliliği planına ilişkin bir test programı ile kurumun tedarikçilerle olan bağımlılık düzeyi tanımlanmış olup tedarikçilerin de katılımıyla periyodik olarak testler gerçekleştirilmektedir.

☐ Kritik tedarikçilerin iş süreklilik planlarının yeterliliği gözden geçirilerek iş süreklilik planına ilişkin olarak en basitinden çeşitli simülasyonların da kullanıldığı en kapsamlı testler periyodik olarak gerçekleştirilmekte ve test sonuçlarına göre planda gerekli aksiyonlar alınmaktadır.

☐ Kurum yılda en az bir kereden az olmamak kaydıyla tedarikçilerinde katılımıyla kapsamlı olarak entegre iş süreklilik planı testi gerçekleştirmekte, test sonuçlarına göre süreçler gözden geçirilip, tedarikçilerin performansları değerlendirilmektedir. Bu test sistem üzerinde yaratılan simülasyonlar ve senaryo analizleri ile gerçekleştirilmektedir.

DF04)Elektronik Veri ve Kritik Dokümanların Yedeklenmesi

Kurumunuz için önemli olan elektronik veri ile basılı formdaki dokümanın yedekleme ve arşivlenme durumunu değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda basılı veya elektronik formdaki verilerin yedeklenmesi konusunda bir farkındalık oluşmamıştır.

☐ Kurum için kritik önemde olan veri ve doküman ile elektronik verinin kurum dışında bir merkezde yedeklenmesine ilişkin bir plan yoktur.

☐ Kritik veri, kayıtlar ile belgeler tanımlanmış,ama bunların yedekleri kurum dışında ayrı bir merkeze gönderilmemekte kurum içinde saklanmaktadır.

☐ Kritik veri ve kayıtların yedekleri ile kritik önemdeki fiziki belge ve kayıtlar taranarak bilgisayar ortamına aktarılmış ve bu taralı dosyalar kurum dışındaki bir merkezde de yedeklenmektedir.

☐ Kritik veri ve kayıtların yedekleri ile kritik önemdeki fiziki belge ve kayıtlar taranarak bilgisayar ortamına aktarılmış olup bunlar kurum dışındaki bir merkezde yedeklenmiştir. Söz konusu merkeze kurum dışındaki farklı bir lokasyondan da erişilebilmekte ve bu durum test edilmektedir.

☐ Kurum içerisindeki iş süreçleri ve fiziki dokümanlar anlık yedekleme gerçekleştiren gelişmiş doküman yönetim sistemi programları vasıtasıyla, veri ise sistem ile senkronize bir şekilde çalışan anlık veri kopyalama sistemleri aracılığıyla ayrı bir merkezde yedeklenmektedir.

DF05)Acil Durum Merkezinin Kurulması

Kurumunuzun acil durum anında operasyonlarını ayrı merkezden yönetebileceği acil durum merkezi konusundaki durumunu değerlendirerek aşağıdaki en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda faaliyetlerin acil durum anında farklı bir merkezden sürdürülmesine imkan tanıyan “Acil Durum Merkezi”nin oluşturulmasına ilişkin bir farkındalık yoktur.

☐ Acil durum anında, kurumun faaliyetlerinin farklı bir merkezden yönetilmesi gerekebileceğine ilişkin kurumsal bir farkındalık sınırlı ölçüde oluşmuştur.

☐ Kurumun kritik iş süreçlerinin farklı bir merkezde yönetilebilmesine imkan tanıyan stratejik kararlar alınmış ve gerekli planlamalar yapılmıştır.

☐ Kurum faaliyetlerinin acil durum anında farklı merkezden sürdürülmesi konusunda bir merkez kiralanmış/satın alınmış ve gerekli teçhizatın bir kısmı sağlanmış fakat henüz test edilmemiştir.

☐ Kurum faaliyetlerinin acil durum anında farklı merkezden sürdürülmesi konusunda bir merkez kiralanmış/satın alınmış bir kısım kritik süreçler için faaliyetin acil durum merkezinden sürdürülmesi testi gerçekleştirilmiştir.

☐ Kurum acil durum merkezini oluşturmuş ve her yıl en az bir kez normal mesai saatleri içerisinde ana merkezdeki sistemini kapatıp faaliyetlerini durdurmakta, acil durum merkezinden yarım kalan faaliyetlerine devam ederek sonlandırma şeklindeki testi başarıyla gerçekleştirmektedir.

DF06)Acil Durum ve İş Süreklilik Eğitimleri

Acil durum ve iş süreklilik planı kapsamında işyeri güvenliğinin sağlanması ve çalışanlara verilen eğitimleri değerlendirerek aşağıdaki en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumda bu konuda bir farkındalık oluşmamıştır.

☐ İşyeri güvenliğinin sağlamasında yasal gereksinimler ve sektörel standartlar göz önünde bulundurulmakta fakat kurumun belirlenmiş bir eğitim programı mevcut değildir.

☐ İşyeri güvenliğinin sağlanmasına yönelik planlamalar, çalışanların sağlık ve güvenlik konusunda farkındalıklarını artırmaya dönük olup "iş süreklilik planı" eğitimleri sadece iş süreklilik yönetim ekibinde yer alan personele verilmektedir.

☐ Çalışanlara işyeri güvenliliğinin sağlanmasına ilişkin yangın, deprem tatbikatları, ilk yardım eğitimleri gibi temel düzeyde "iş süreklilik yönetimi eğitimleri" verilmekte olup katılım zorunlu tutulmamaktadır.

☐ İş süreklilik planında görev alan kilit personel belirlenmiş, ihtiyaçlar ve sorumluluk alanları doğrultusunda eğitimlere katılmaları zorunlu tutulmuş olup her yıl belirli dönemlerde acil durum ve kurtarma tatbikatları gerçekleştirilmektedir.

☐ Kurumda çalışanlara yönelik olarak periyodik bir şekilde, iş süreklilik yönetimine, iş yeri güvenliği ve can güvenliğinin sağlanmasına ilişkin kapsamlı ve ihtiyaca dönük eğitimler bu konuda uzman kuruluşlarca verilmekte ve sağlanan katkı, yapılan tatbikatlar ve sınavlarla ölçülmektedir.

DF07)Fiziksel ve Çevresel Güvenlik

Kurumunuzun fiziksel ve çevresel güvenliğini değerlendirerek size en uygun seçeneği (X) ile işaretleyiniz.

☐ Kurumun varlık ve uygulamalarının korunması, nem, duman, toz, sıcaklık gibi çevresel faktörlerin ölçülmesi ve kontrol edilmesi konusundaki bilinci tamamıyla oluşmamıştır.

☐ Yönetim, banka personelini, varlıklarını ve uygulamalarını korumak, doğal afetler ve insan kaynaklı zararlar karşısında güvenilir bir çalışma ortamı tesis etmek konusunda farkındalık sahibi olmasına karşın bazı önemli varlık ve uygulamaların korunması ve yönetimi birkaç personelin bireysel yetenek ve tecrübesine bağlı durumdadır.

☐ Banka varlıklarının fiziksel ve çevresel güvenliğinin sağlanması ve izlenmesine dönük hedefler konusunda prosedürler yeterince dokümante edilmemiş; güvenlik, operasyonları gerçekleştiren birimlerin bireysel yeteneklerine bırakılmış durumdadır.

☐ Fiziksel ve çevresel güvenliğin sağlanmış olduğu bir çalışma ortamının gerekliliği kurumsal olarak kabul edilmiş, bunun için bütçe ayrılmış olup çalışma alanının sağlığı ve güvenliği yasal mercilerce denetlenmektedir.

☐ Çevresel ve fiziksel güvenliğin önemi, personele kurum çapında verilen sağlık, sivil savunma ve gerekli diğer zorunlu eğitimlerle tamamen anlaşılmış olup, varlıkların sahip ve sorumluları belirlenerek bunlara erişimler kontrol edilmekte, güvenlik seviyeleri belirlenmiş metriklerle ölçülerek yönetim tarafından izlenip değerlendirilmektedir.

☐ Fiziksel ve çevresel güvenlik, iş süreklilik ve kriz yönetimi politikalarıyla uyumlu olacak şekilde prosedüre edilmiş olup, özel araçlar ve teknolojiler kullanılarak test edilmekte, belirlenen metriklerle ölçülüp izlenerek yönetim tarafından değerlendirilip optimize edilmektedir.

KAYNAKÇA

"Bilişim Sistemleri Güvenliği El Kitabı"**, TBD Kamu-BİB Bilişim Platformu**, http://kamubib.tbd.org.tr/dokumanlar/bg2.doc (22 Mart 2007).

"Bilişim Teknolojilerinde Risk yönetimi"**, TBD Kamu-BİB Kamu Bilişim Platformu VIII**, 2.Çalışma Grubu Raporu, Belge No: ÇG2/Sürüm4, http://www.kamubib.tbd.org.tr/dokumanlar/CG2S.doc (22 Mart 2007).

"Enterprise-wide Risk Management for Insurance Industry", Global Study, PWC,2004.

"Guidelines for the Security of Information Systems", http://www.oecd.org 1992.

ACT Insurance Authority, "Guide to Risk Management", 2004, http://www.treasury.act.gov.au/actia/Guide.doc (13 Temmuz 2008).

Acuner, Şebnem. "İnsan Kaynaklı Davranışşal Riskler ve Kuruluşlara Maliyeti", **Active**, May-Haz 2006.

Akal, Zuhal. **"İşletmelerde Performans Ölçüm ve Denetimi; Çok Yönlü Performans Göstergeleri"**, Ankara: MPM Yayını, 1992.

Akkizidis Ioannis and Vivianne Bouchereau. http://www.ffiec.gov/ffiecinfobase/booklets, (19 Ocak 2007).

Akkizidis, Ioannis and Vivianne Bouchereau. **Guide to Optimal Operational Risk and Basel II**, New York:Auercbach Pub., 2006ve Bouchereau.

Aktan, Can. "2000'li Yıllarda Yeni Yönetim Teknikleri: İnsan Mühendisliği", İstanbul: TÜGİAD Yayını, 1999.

Alberts, Christopher and Audrey Dorofee. **OCTAVE Method Implementation Guide Vol.18 Appendix/E**, Pittsburgh: Carnegie Mellon Software Engineering Institute, 2003.

Alexander, Carol. **Operational Risk: Regulation, Analysis and Management,** London ; New York:Financial Times Prentice Hall, 2003.

Altıntaş, M.Ayhan. **Bankacılıkta Risk Yönetimi ve Sermaye Yeterliliği**, Ankara:Turhan Kitabevi, 2006.

Ansell, Jake ve Frank Wharton. **Risk: Analysis, Assessment and Management**, John Wiley and Sons, 1992, s.4-5'den Arman T.Tevfik, **Risk Analizine Giriş**, 1.Baskı, İstanbul: Alfa Basım Yayım Dağıtım, 1997.

ARME soruyor/**ActiveAcademy**, "Risk yönetimi, kurumsal yönetimin bir parçasıdır." Tamer Saka ile mülakat.

Artinyan, Elize Natasa. " COBIT Çerçevesi", **Active Dergisi**, Sayı.54, 2007.

Avrupa Komisyonu, "Banking Supervision:Reform of the Capital Adequacy Framework-Frequently Asked Questions", 2001, http://europa.eu/old-address.htm, (17 Temmuz 2007).

Avrupa Komisyonu, "Working Document of the Commission Services on Capital Requirements for Credit Institutions and Investment Firms", 2002, http://europa.eu/old-address.htm, (16 Kasım 2007).

Babuşçu, Şenol. **Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi**, Ankara: Akademi Consulting&Training, Eylül 2005.

Baltaş, Acar. **Değişimin İçinden Geleceğe Doğru Ekip Oluşturma ve Liderlik**, İstanbul:Remzi Kitapevi, Aralık 2000.

Bankacılar Dergisi, Operasyonel Risk Çalışma Grubu, "Operasyonel Risk İleri Ölçüm Yaklaşımları Kullanılarak Ekonomik Sermaye Hesaplaması, İleri Ölçüm Yaklaşımları-Ekonomik Sermaye İlişkisi",TBB, 2006, Sayı.58.

Bankacılar Dergisi, Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, "Operasyonel Risk Veri Tabanı",TBB, Haziran 2004, Sayı.48.

Bankacılar Dergisi, Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, "Operasyonel Risk Veri Tabanı", TBB, Nisan 2004.

Bankacılar Dergisi, Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu, "Bankalar İçin Acil Durum ve İş Süreklilik Planlaması", Türkiye Bankalar Birliği, Eylül 2002, Sayı 42, s.26; ARME, Sayı 5.

Barman,Scott. **Writing Information Security Policies**, New Riders Publishing, 2001'den Günce Öztürk.

Baş, Türker ve Murat Oymak. **ISO 9001:2000 Kalite Yönetim Sistemi**, 3.Baskı, Ankara:Seçkin Yayıncılık, 2007.

Baş, Türker. **Anket Nasıl Hazırlanır, Uygulanır, Değerlendirilir?**, 4.Baskı, Ankara:Seçkin Yayıncılık, Ocak 2006.

Bayoğlu, Burak. **Bilgi Güvenliği Yönetim Sistemi Uygulama ve Denetleme Semineri Notları**, Takasbank (Aralık 2008), TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Bayram, Nuran. **Sosyal Bilimlerde SPSS ile Veri Analizi,** 1.Baskı, Bursa:Ezgi Kitabevi, 2004.

BCBS, "Framework For Internal Control Systems in Banking Organization." September 1998, No.40, http://www.bis.org/publ/bcbs40.pdf, (14 Eylül 2008).

BCBS, "High-level Principles for Business Continuity" , The Joint Forum, 2005. http://www.cnmv.es/publicaciones/IOSCOPD224.pdf (11 Ağustos 2007).

BCBS, "International Convergence of Capital Markets and Capital Standards,A Revised Framework Comprehensive Version", 2004, http://www.bis.org/publ/bcbs107.pdf (19 Şubat 2008).

BCBS, "Overview of the Amendment to the Capital Accord to Incorporate Market Risks", 1996, http://www.bis.org/publ/bcbs23.htm (13 Nisan 2007).

BCBS, “Risk Management Principles for Electronic Banking”, Temmuz 2003.

BCBS, “Sound Practices For the Management and Supervision of Operational Risk”, December 2001.

BCBS, “Working Paper on the Regulatory Treatment of Operational Risk”, 2001, http://www.bis.org/publ/bcbs_wp8.pdf?noframes=1 (23 Temmuz 2007).

BCBS, Bank For International Settlements, “Framework For Internal Control Systems in Banking Organization.” September 1998, No.40, http://www.bis.org/publ/bcbs40.pdf (14 Eylül 2008).

BCBS. “A New Capital Adequacy Framework, Consultative Paper”, 1999, http://www.bis.org/, (17 Ocak 2008).

BCBS. “Operational Risk Management”, 1998, http://www.bis.org/, (28 Mart 2008).

BCBS. “Operational Risk, Consultative Document”, 2001, http://www.bis.org/.

BCBS. “Risk Management Guidelenes for Derivatives”, 1994, http://www.bis.org/, (19 Mart 2008).

BDDK Aylık Bülten, Mayıs 2009. http://www.bddk.org.tr/WebSitesi/turkce/Istatistiki_Veriler/Aylik_Raporlar/6426Aylik_Bulten_Mayis2009.pdf

BDDK Finansal Piyasalar Raporu, Sayı.12, Aralık 2008. http://www.bddk.org.tr/WebSitesi/turkce/Raporlar/Finansal_Piyasalar_Raporlari/6320Finansal_Piyasalar_Raporu_Aralik_2008.pdf (12 Mart 2009).

BDDK, “Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik”, 01/11/2006 tarih ve 26333 sayılı Resmi Gazete, (Md:21).

BDDK, **Bankacılık Sektörü Basel II İlerleme Raporu**, Mayıs 2009.

BDDK. “Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmeliğin Uygulanmasına İlişkin 1 Sayılı Tebliğ”, 2002, http://www.bddk.org.tr/, (17 Ekim 2008).

BDDK. “Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmelik”, 2001, http://www.bddk.org.tr/, (17 Ekim 2008).

BDDK. “BDDK tarafından T.Bankalar Birliği Genel Sekreterliğine gönderilen 03.10.2001 tarih ve BDDK.RGTAD.-II.1-8111 sayılı yazı ve eki açıklama”**,** 2001, http://www.bddk.org.tr/, (16 Aralık 2007).

Berk, Niyazi. **Bankacılıkta Pazara Yönelik Kredi Yönetimi**, 3.basım, İstanbul: Beta Basım Yayın Dağıtım, Mart 2001.

Berk, Niyazi. **Finansal Yönetim**, 7.baskı. İstanbul: Türkmen Kitabevi, 2003.

BIS. “Focused Seminar On Operational Risk”: Basel, 16 -17 July 2002. Switzerland: Financial Stability Institute.Bank For International Settlements, 2002.

Bidgoli, Hossein ve Reza Azarmsa, Computer Security. “New Management Concern For The 1980s And Beyond”, **Journal of Systems Management**, (October 1989), s.21’den Tamer Saka, **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi**, TBB, İstanbul, 2001.

Bilgin, Mehmet Hüseyin. “Bireysel Performansa Dayalı Ücret ve Verimlilik”, http://www.econturk.org/Turkiyeekonomisi/cmis1.pdf (12 Haziran 2009).

Bolgün, K. Evren ve M.Barış Akçay. **Risk Yönetimi Gelişmekte Olan Türk Finans Piyasasında Entegre Risk Ölçüm ve Yönetim Uygulamaları,** 2.Baskı, İstanbul:Scala Yayıncılık, Haziran 2005.

Bologna, G.Jack, Robert J.Lindquist ve Joseph T.Well. **“The Accountant’s Handbook of Fraud and Commercial Crime”**, John Willey&Sons, 1993, s.190’dan Tamer Saka, **“Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi”**, TBB, İstanbul, 2001.

Booker, Shirley ve Diğerleri. “What Is Your Risk Appetite? The Risk-IT Model”, **Information Systems Control Journal**, Volume 2 , 2004, http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18439 (12 Kasım 2008).

Bozkurt, Ünal. **İşletme Finansının Temelleri**, İstanbul: Literatür Yayıncılık, Ekim 1997, s.251’den Engin Kurun, **Faiz Riski Yönetimi ve Türkiye Uygulaması**, 1.Baskı, Sermaye Piyasası Kurulu, yayın no:181, Ankara:2005.

Brink, Gerrit Jan van den. **Operational Risk, The New Challenge for Banks,** 1.Baskı, New York:Palgrave Publishers Ltd., 2002.

Buchelt, R ve S. Unteregger. “Cultural Risk and Risk Culture: Operational Risk After Basel II”**,** 2004, Financial Stability Report 6’dan Moosa.

Can, Evrim. “Operasyonel Risk ve Yönetimi”, **SPK Yeterlik Etüdü**, Yayın No.154, Ankara: 2003.

Candan, Hasan ve Alper Özün. **Bankalarda Risk Yönetimi ve Basel II**, 1.Baskı, İstanbul:T.İş Bankası Kültür Yayınları, 2006.

Capezio, P. ve D. Morehouse. **Taking the Mystery out of TQM,** Career Press, 1995’den Smith, Clifford, **Total Quality Managmenet**.

Carreño, M.L., O.D. Cardona, ve A.H. Barbat. “Evaluation of the Risk Management Performance”, 250th Anniversary Of The 1755 Lisbon Earthquake, 2005. http://www.unisdr.org/HFdialogue/download/tp1-Evaluation-risk-management-performance-m1.pdf (Şubat 2009).

Cenk, Ali Kemal. “Uluslararası Bankacılık Denetim İlkeleri ve Denetim Süreçleri”, **Active Finans**, Mart-Nisan 2005.

Chambers, Nurgül ve Atilla Çifter. “Operasyonel Risk Yönetiminde Zarar Dağılımları İle Gelişmiş Ölçüm Yaklaşımı Uygulaması”, **Doğuş Üniversite Dergisi**, 8, (2), (2007).

Chapman, Robert J**. Simple Tools and Techniques for Enterprise Risk Management**, 2006.

Chorafas, Dimitris N. **Operational Risk Control With Basel II: Basic Principles&Capital Requirements,** Boston:Elsevier Butterworth-Heinemann, 2004.

COBIT 4.1, IT Governance Insitute, http://isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/Obtain_COBIT.htm

Committee of Sponsoring Organizations of the Treadway Commission (COSO), **Enterprise Risk Management Integrated Framework, Executive Summary Framework,** New York, AICPA, September 2004.

Connel, Patrick Mc. "A Standards Based approach to Operational Risk Management", http://www.continuitycentral.com/ORStandards.pdf (14 Temmuz 2008).

Crouhy, Michel, Dan Galai ve Robert Mark. **Risk Management [electronic resource],** New York: McGraw Hill, 2000.

Çalışkan, Gülay. "Altı Sigma ve Toplam Kalite Yönetimi", **Elektronik Sosyal Bilimler Dergisi**, 2006-Yaz, C.5, S.17.

Davis, Gordon B., Donald L Adams ve Carol A. Achaller. **Auditing&EDP**, AICRA, 1983, s.127-128'den Tamer Saka.

Deregözü, Rıfat. **"Bankacılıkta Bilgi Sistemleri Denetim- BDDK Yaklaşımı ve Bilgi Güvenliği",** Tübitak UEKAE Bilgi Teknolojileri Güvenliği Konferansı, İstanbul: Harbiye Askeri Müzesi, 13-14 Mart 2008.

Dowd, V. "Measurement of Operational Risk: The Basel Approach", Carol Alexander (Ed.), **Operational Risk: Regulation, Analysis and Management**, London,2003, PrenticeHall.

Down, Kevin. **Beyond Value At Risk,** Sussex:John Willey&Sons, 1998.

Drougou, Edouard. “IT Governance at a Financial Institution”, **(Yayınlanmamış Master Thesis, KTH Electirical Engineering, Stockholm).**

Eke, Selda. “Risk Yönetimi ve Risk Yönetiminin Kurumsal Yönetim İlkeleri Açısından Önemi” **ActiveFinans**, Mart-Nisan 2005.

Eken, M.Hasan ve Hüseyin Selimler. **Banka Muhasebesi**, İstanbul: Der Yayınları, 2004.

Eken, M.Hasan. “Basel II ve Risk Yönetimi”, http://www.tkyd.org/files/downloads/mehmet_hasan_eken_basel_ii.pdf (20 Şubat 2009).

Eskiyörük, Doğan. “BGYS – Risk Yönetim Süreci Kılavuzu”, **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00,17/08/2007, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0004-bgys-risk-yonetim-sureci-kilavuzu.html (16 Haziran 2008).

FAA System Safety Handbook, Types of Risk Defined, Operational Risk Management. http://www.faa.gov/library/manuals, (13 Nisan 2008).

FFIEC “Business Continuity Planning: IT Examination Handbook”, 2003.

FFIEC- Fedaral Financial Institutions Examination Council, **Information Systems Examination Handbook**,1996, s.10’den Tamer Saka, **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi**, TBB, İstanbul, 2001.

Frost, Chris, David Allen, James Porter and Philip Bloodworth. **Operational Risk and Resilience,** Boston:Butterworth-Heinemann, 2001.

G.Cruz, Marcelo. **Operational Risk Modeling Theory and Practice**, Navara:Risk Books, 2004.

Gallagher, R.B. “Risk Management: New Phase of Cost Control”, **Harvard Business Review**, (Sep-Oct. 1956)’den Imad A. Moosa, **Operational Risk Management**, Eeastbourne:Palgrave Macmillan, 2007.

Gegez, A. Ercan. **Pazarlama Araştırmaları,** 1.Baskı, İstanbul: Beta Yayınevi, 2005.

Griffiths, David. "Risk Based Internal Auditing", 15/03/2006, Version:2.0.3, http://www.internalaudit.biz/files/implementation/Implementing%20RBIA%20v1.1.pdf (14 Şubat 2007).

GTAG, "**Bilgi Teknolojisi Kontrolleri**", Uluslararası İç Denetim Enstitüsü, http://www.tide.org.tr/tideweb/resimler/upload/Documents/GTAG, (16 Haziran 2008).

GTAG, Global Teknoloji Denetim Kılavuzu, "Bilgi Teknolojisi Kontrolleri", **IIA: Uluslararası İç Denetçiler Enstitüsü**, ,2005, http://www.tide.org.tr/tideweb/resimler/upload/Documents/GTAG, (16 Haziran 2008).

Guldentops, Erik, Wim Van Grembergen ve De Haes Steven. "Control and Governance Maturity Survey: Establishing a Reference Benchmark and a Self-assessment Tool", **Information Systems Control Journal**, Volume 6, (2002), http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16122&TEMPLATE=/ContentManagement/ContentDisplay.cfm (15 Ocak 2009).

Güler, Fazıl. **İstatistik Metodları ve Uygulamaları**, İstanbul:Beta, 2005.

Haubenstock, Micheal. "The Operational Risk Management Framework", Carol Alexander (Ed.), **Operational Risk Regularion, Analysis and management**, London:Prentice Hall, 2003.

Hoffman, Douglas G. **Managing Operational Risk: 20 Firmwide Best Practice Strategies,** New York:Wiley, 2002.

Horcher, Karen A. **Essentials of Financial Risk Management,** Hoboken, NJ, USA: John Wiley&Sons, Incorporated, 2005, http://site.ebrary.com/lib/boğazici (12 Eylül 2007).

http://www.bilgiguvenligi.gov.tr

http://www.bis.org/bcbs/index.htm (27 Haziran 2009).

http://www.canaktan.org

http://www.canaktan.org/yonetim/insan-yonetim/motivasyon-teorileri.htm (17 Haziran 2008).

http://www.erisk.com

http://www.ferma-asso.org

http://www.ffiec.gov/ffiecinfobase/booklets,

http://www.garp.com

http://www.iaa.org.uk

http://www.internalaudit.biz

http://www.iosco.org/about/

http://www.isaca.org

http://www.kendinigelistir.com/peter-druckerin-hayatindaki-7-onemli-ders/ (12 Mayıs 2007).

http://www.makelem.com

http://www.rims.org

http://www.riskyonetimi.com

http://www.tbb.org.tr

http://www.theiia.org

http://www.tide.org.tr

http://www.tkbb.org.tr/

Humphreys, Ted ve Angelika Plate. **Guide to the Implementationn and Auditing of ISMS Controls based on ISO/IEC 27001**, British Standards Institution, 2005'den Günce Öztürk.

Humphreys, Ted. "ISMS Standarts The ISO 27000 Family and BS7799-2"**, ISMS International User Group Seminar**, s.32-35'den Ünal Perendi.

Hussain, Amanat. **Managing Operational Risk in Financial Markets,** Oxford; Boston: Butterworth-Heinemann, 2000, s.70-71.

Hübner, Robert, Mark Laycock&Fred Peemöller. "Managing Operational Risk", **"Advances in Operational Risk Firm-wide Issues for Financial Institutions"**, London: Risk Boks, 2001.

Information Security Magazine / http://www.infosecuritymag.com, (17 Eylül 2008).

IOSCO. "Risk Management and for Securuities Firms and Their Supervisors"**, A Report by the Technical Committee of The IOSCO,** 1998, http://www.iosco.org, (11 Kasım 2007).

Ishikawa,Karou. **What is Total Quality Control: The Japanesse Way**, Londra, Printece Hall, 1985'den Dikmen, M.K. ve Dikmen, A.A, "Her Derde Deva İksir: Toplam Kalite Yönetimi", http://www.tkgm.gov.tr/turkce/dosyalar (07 Temmuz 2008).

ITGI ve OGC, **"Aligning COBIT,ITIL, and ISO 17799 for Business Benefits:Management Summary"**, 2005, http://www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf (19 Haziran 2008).

İbiş, Cemal ve Ayça Akarçay. "IOSCO Deklarasyonu ve Menkul Kıymet Borsalarında IAS'ın Uygulanması Süreci", Marmara Üniversitesi, İİBF.

İç Denetim Dergisi, "İş Sürekliliği Planlaması" Kış 2003, s.55; Down.

İç Denetim Dergisi, Matthew Collins ile Röportaj. Çev. Evren Altıok "İş Sürekliliği Planlaması" Kış 2003, Sayı.6, s.54-55.

Jorion, Philippe. **Value at Risk [electronic resource]: The New Benchmark For Managing Financial Risk,** New York: McGraw-Hill, c2001.

Kaval, Hasan. **Bankalarda Risk Yönetimi,** Ankara:Yaklaşım Yayınları, 2004.

Kayım, Ali. "Kurumsal Risk Yönetimi ve İç Denetimin Kurumsal Risk Yönetimindeki Yeri", **ActiveFinans**, Ekim-Aralık,2006.

Keenan, Kate. **The Managment Guide to Selecting People**, Sussex:Ravette Books, 1995.

Khan, Ali Samad. **"Data Modeling",** Presentation in *How to Master and Quantify Operational Risk, The GARP Operational Risk Seminar,* 18-19 October 2001, London'dan Mazıbaş, "Bankalarda Operasyonel Risk Veri Tabanının Oluşturulması".

King, Jack L. **Operational Risk: Measurement and Modelling,** John Willey and Sons, Sussex: 2001.

Koç, Fatih. "BGYS – Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu", **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0003-varlik-envanteri-olusturma-kilavuzu.html (20 Mart 2008).

Kul, Altuğ. "COBIT'te Olgunluk Seviyelerinin Anlamı ve Hesaplanması", Deloitte Kurumsal Hizmetler Yayını, http://www.denetimnet.net/UserFiles/Documents/DeloitteMakaleleri/Altu%C4%9F_Kul_Makale_Haziran_2007.pdf (12 Haziran 2007).

Kurtuluş, Naciye ve Müge Aşlan. **Risk Odaklı İç Denetim Konferansı**, DEVAK Deloitte Academy, 18-19 Haziran 2008, Ritz Carlton, İstanbul.

Lainhart, J.W. (2001) "COBIT Management Guidelines IT Governance Forum Trust and Understanding for the Business and the Board", ITGI Paris.

Lam, James. **Enterprise Risk Management: From Incentives to Controls,** John Wiley and Sons, 2003.

LLOYD'S, "Risk Management Toolkit", http://www.lloyds.com/Lloyds_Market/Tools_and_reference/Risk_Management_Toolkit_home/ (12 Mart 2007).

Marshall, Christopher Lee. **Measuring And Managing OPERATIONAL RISKS in Financial Institutions: Tools,Techniques and Other Resources**, Singapore: John Wiley&Sons, 2001.

Mazıbaş, Murat. "Bankalarda Operasyonel Risk Veri Tabanının Oluşturulması", **BDDK Çalışma Raporları,** Mart 2006.

Mazıbaş, Murat. "Operasyonel Riske Bazel Yaklaşımı: Üç Yapısal Blok Çerçevesinde Bir Değerlendirme", **BDDK Araştırma Raporları**, 2005/1.

Moller, Robert. **Brink's Modern Internal Auditing**, New Jersey:John Willey, 2005.

Moosa, Imad A. **Operational Risk Management**, Eeastbourne:Palgrave Macmillan, 2007.

Morrion, Alan D**.** "Sarbanes Oxley, Corporate Governance and Operational Risk" **Sarbanes-Oxley Seminar**, 22 Temmuz 2004.

Murphy, Michael A. ve Xenia Ley Parker. **Handbook of EDP Auditing, 1994 Cumulative Supplement**, Coopers&Lybrand 1994, s.37-38'den Tamer Saka.

Nakıp, Mahir. **Pazarlama Araştırmaları ,Teknikler ve Uygulamalar,** 2.Baskı, Ankara: Seçkin Yayınevi, 2006.

Nash, R.A. "The Three Pillars of Operational Risk", Carol Alexander (Ed.), **Operational Risk: Regulation, Analysis and Management**, London,2003, PrenticeHall.

Negron, Thomas. "Audit Concerns in the PC Environment", Internal Auditing, Winter 1992, s.38-43'den Tamer Saka.

Olsson, Carl. **Risk Management in Emerging Markets**, 1.Baskı, London:Prentice Hall, 2002.

OTUZLAR GRUBU**.** "Derivatives Practices and Principles, Global Derivatives Study Group"**, ORRF (Operational Risk Researh Forum),** 1993, http://www.group30.org/ (31 Aralık 2006).

OTUZLAR GRUBU. **"Insurance as a Mitigant For Operational Risk",** A Report Submitted to the Basel Committee on Banking Supervision by the Insurance Working Group of the ORRF, 2001, www.orrf.org, (22 Temmuz 2007).

Önel, Dinçer ve Ali Dinçkan. "Bilgi Güvenliği Yönetim Sistemi Kurulumu" **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00,28/08/2007, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulum-kilavuzu.html (16 Haziran 2008).

Özdamar, Kazım. **Paket Programlar İle İstatistiksel Veri Analizi (Çok Değişkenli Analizler)**, 4.Baskı, Eskişehir:Kaan Kitabevi, 2002.

Özkul, Levent. **ABD Sermaye Piyasalarında Yaşanan Son Gelişmeler ve ABD'de Yürürlüğe Giren 2002 Tarihli Sarbanes-Oxley Kanunu'nun Türk Sermaye Piyasası Açısından Değerlendirmesi**, Sermaye Piyasası Kurulu, Yayın No:166, Ankara:2002.

Özmen, Kemal. **"Bilgi İşlem Risk Yönetimi"**, http://www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=279 (21 Mayıs 2008).

P. Mestchian, "Operational Risk Management: The Solution is in the Problem, in Advances in Operational Risk: Firm-Wide Issues for Financial Institutions, London:Risk Boks, 2003'den Moosa.

Pande, Peter S., Robert P. Neuman, Roland R. Cacanagh. **The Six Sigma Way, 2000**, Çev. Nafiz Güder ve Güneş Tokcan, **Six Sigma Yolu**, 1.Basım, İstanbul: Klan Yayınları, 2003.

Paulk, Mark C., Charles V Weber ve Mary Beth Chrisis. "**The Capability Maturity Model for Software**" http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr24.93.pdf (19 Mart 2009).

Peltier, Thomas R. &Justin Peltier. **Complete Guide to CISM Certification**, New York: Auerbach Publications, 2006.

Raz, T. ve D. Hillson. "A Comparative Review of Risk Managemenet Standards", Risk Management: **An International Journal,** 7 (4), (2005).

Risk yöneticileri Derneği Bülteni, "Operasyonel Risklerin Kontrol Edilmesi ve/veya Azaltılmasına Yönelik Faaliyetler", Eylül 2004.

Risk Yönetimi ve Basel 2'nin Kobi'lere Etkileri, İstanbul: Türkiye Bankalar Birliği, 2004.

Saaty, T.L. **Analytical Planning**, RWS Publications, 1985.

Saaty, T.L. **Fundamentals of Decision Making and Priority Theory with Analytic Hierarchy Process**, AHP Series, Vol: VI, RWS Publications, 2000.

Saka,Tamer. **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi**, TBB, İstanbul, 2001.

Saliba, R**.** "Callio Secura 17799- A tool for Implementing the ISO 17799/BS 7799", 1998, s.12-14'den Ünal Perendi**,** "BGYS Kapsamı Belirleme Kılavuzu", **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00, 21/03/2008, http://www.bilgiguvenligi.gov.tr (16 Haziran 2008).

Salle, Mathias. "**IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing**" HP Laboraitories Palo Alto, 2004, s.4. http://www.hpl.hp.com/techreports/2004/HPL-2004-98.html (14 Ağustos 2008).

Sampson, G., D. Kumar ve D. Lau Andersen. “Firmwide Issues for Financial Institutions: Risk Model Selection”, Sarah Jenkins(Ed.), **Advances inOperational Risk Firm-wide Issues for Financial Institutions**, Somerset:RiskBooks, 2001.

Sipahi, Beril, E.Serra Yurtkoru ve Murat Çinko. **Sosyal Bilimlerde SPSS’le Veri Analizi**, 2.Baskı, İstanbul:Beta Yayınları, 2008.

SPSS 13.0 for Windows, User’s Guide.

Steiguer, J.E. De,Jennifer Duberstein ve Vicente Lopes. “The Analytic Hierarchy Process as a Means for Integrated Watershed Management”**,** http://www.tucson.ars.ag.gov/ICRW/Proceedings/Steiguer.pdf (20 Mart 2009).

Şencan, Hüner. **Sosyal ve Davranışsal Ölçümlerde Güvenilirlik ve Geçerlilik**, 1.Baskı, Ankara:Seçkin Yayıncılık, Ocak 2005.

T.İş Bankası Risk Yönetim Müdürlüğü, **Bankacılıkta Yeni Sermaye Yeterliliği Düzenlemeleri: Basel-II,** T.İş Bankası Yayın No:78, 2004.

Takan, Mehmet. **Bankalarda Toplam Kalite Yönetimi,** TBB Yayın 217, İstanbul, 2000.

Tanju, Yavuz Salih. “İç Kontrol Fonksiyonun Bileşenleri, İç Kontrol Merkezi Teftişten Farklı Bir Mekanizmadır”**,** TBB, **Bankacılar Dergisi**, Sayı.42, 2002.

Tatlıdil, Hüseyin. **Uygulamalı Çok Değişkenli İstatistiksel Analiz**, Ankara:Akademi Matbaası, 2002.

Teker, Dilek Leblebici. “Bankacılıkta Operasyonel Risk Ölçüm Modelleri Ve Sermaye Yeterliliğine Etkisi: Türk Bankacılık Sektöründe Faaliyet Gösteren Bir Bankaya Uygulanması”, **Yayımlanmamış Doktora** Tezi. İTÜ Sosyal Bilimler Enstitüsü, 2005.

Teker, Dilek Leblebici. **Bankalarda Operasyonel Risk Yönetimi Örnek Banka Uygulamalı,** 1.Baskı, İstanbul:Literatür Yayınları, 2006.

Teker, Dilek. “Bankacılıkta Operasyonel Risk Ölçüm Modelleri Ve Sermaye Yeterlilik Oranına Etkisi”, Türkiye Bankalar Birliği Eğitim ve Tanıtım Grubu seminer notları, İstanbul 20-21 Ekim 2005.

Tevfik, Arman. **Risk Analizine Giriş,** 1.Baskı, İstanbul: Alfa Basım Yayım Dağıtım, 1997.

The Banker’s Guide to The Basel-II Framework, The Banking Association of South Africa, 2005, http://www.standardbank.co.za/SB_FILES/BGPsite_2008/The_Bankers_Guide_to_Basel_II.pdf (6 Mart 2007).

The Orange Book, Management of Risk-Principles and Concepts,2004, HM Treasury, http://alberta.ca/home/documents/orange_book_mgmt_risk.pdf, (10 Ağustos 2006).

Tuğlular, Tuğkan. "Üniversitelerde Bilgi Güvenliği Politikaları"**, Ulaknet Sistem Yönetimi Konferansı - Güvenlik**, Ekim 2003’den Günce Öztürk, “Bilgi Güvenliği Oluşturma Kılavuzu”, **TÜBİTAK UEKAE:Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü**, Sürüm 1.00, 21/03/2008, http://www.bilgiguvenligi.gov.tr (16 Haziran 2008).

Uludağ, İlhan ve Erişah Arıcan. **Finansal Piyasalar Ekonomisi (Piyasalar-Kurumlar-Araçlar)**, İstanbul:Beta Yayınları, 1999.

Vinella, Peter ve Jeanette Jin. “A Foundation for KPI and KRI”, Ellen Davis (Ed.), **Operational Risk Practical Approaches to Implementation**, Navara:Risk Books, 2005.

Wruck, K.H ve M. Jensen. “Science, Specific Knowledge and Total Quality Management”, **Journal of Accounting and Economics**, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=55993 (12 Şubat 2008).

Yurtsever, Gürdoğan. “Bankacılıkta Personel Suiistimalerinin Önlenmesi ve Tespiti”, **Active**, Sayı.46, 2006.