T.C.
MARMARA ÜNİVERSİTESİ
BANKACILIK VE SİGORTACILIK ENSTİTÜSÜ
BANKACILIK ANABİLİM DALI

BANKACILIKTA COSO ve COBIT MODELLERİNE GÖRE RİSK MATRİSİNİN OLUŞTURULMASI: BİREYSEL KREDİLER SÜRECİNE İLİŞKİN BİR UYGULAMA

Doktora Tezi

BORA DEDE

İSTANBUL, 2016

T.C.

MARMARA ÜNİVERSİTESİ
BANKACILIK VE SİGORTACILIK ENSTİTÜSÜ
BANKACILIK ANABİLİM DALI

BANKACILIKTA COSO ve COBIT MODELLERİNE GÖRE RİSK MATRİSİNİN OLUŞTURULMASI: BİREYSEL KREDİLER SÜRECİNE İLİŞKİN BİR UYGULAMA

Doktora Tezi

BORA DEDE

Danışman: PROF.DR. CEMAL İBİŞ

İSTANBUL, 2016

T.C.
MARMARA ÜNİVERSİTESİ
Bankacılık ve Sigortacılık Enstitüsü

Aşağıda belirtilen lisansüstü tez, Lisansüstü Öğretim Yönetmeliği hükümlerinde belirtilen esaslar çerçevesinde jüri önünde savunulmuş ve jüri tarafından başarılı bulunmuştur.

TEZ BAŞLIĞI	: Bankacılıkta COSO ve COBIT Modellerine Göre Risk Matrisinin Oluşturulması: Bireysel Krediler Sürecine İlişkin Bir Uygulama
TEZ TÜRÜ	: Doktora
TEZİ HAZIRLAYAN	: Bora DEDE
ANABİLİM DALI	: Bankacılık
SAVUNMA TARİHİ	: 20.12.2016

JÜRİ ÜYELERİ

GÖREVİ	ADI SOYADI	İmza
Danışman	Prof.Dr.Cemal İBİŞ	
Üye	Prof.Dr.Erişah ARICAN	
Üye	Prof.Dr.Hayri KOZANOĞLU	
Üye	Prof.Dr.Serhat YANIK	
Üye	Doç.Dr.Özgür ÇATIKKAŞ	

Marmara Üniversitesi Göztepe Kampusu Bankacılık ve Sigortacılık Enstitüsü 34722 Kadıköy / İSTANBUL
0 (216) 347 69 51 (Faks)
0 (216) 418 20 88
bse@marmara.edu.tr
http://bse.marmara.edu.tr
Ayrıntılı bilgi için: İ.SOYADI Bilgisayar İşletmeni Cemal KURŞUN

ÖZET

BANKACILIKTA COSO ve COBIT MODELLERİNE GÖRE RİSK MATRİSİNİN OLUŞTURULMASI: BİREYSEL KREDİLER SÜRECİNE İLİŞKİN BİR UYGULAMA

Yürütülen faaliyet ve operasyonlarda ortaya çıkan gelişmeler ve değişiklikler, işletmenin kontrol ortamına ait denetim kapsamını da etkilemiş olup, bilgi sistemleri denetiminin öneminin artmasına neden olmuştur. Diğer bir ifadeyle, işletmenin iş süreçleri kapsamında bir değişiklik olmasa bile bilgi teknolojilerinin kullanımının artması, faaliyetlerin yürütülme şeklini, karmaşıklığını ve iş süreçleri üzerindeki kontrol noktalarını etkilediği gibi bu faaliyetlerin denetim sürecini de etkilemiştir.

Çalışma içerisinde bankalarda bireysel kredi faaliyetleri kapsamında yürütülen temel ve alt süreçler incelenmiş, operasyonlarda yer alan anahtar riskler kalitatif yöntem kullanarak tanımlanmıştır. Tanımlanmış olan riskleri minimize edecek olan kontrol faaliyetleri tespit edilerek risk matrisi oluşturulmuştur. Bu çalışmanın konusu, operasyonel ve bilgi teknolojilerine ait risklerin, bir bankaya ait operasyonel faaliyetleri üzerindeki etkilerinin yönetilmesi ve kontrol edilmesi amacıyla risk matrislerinin COSO ve COBIT kontrol modellerine göre nasıl oluşturulması gerektiği yönünde bir öneride bulunmak ve fikir vermektir.

Çalışmanın amacı, bağımsız denetim faaliyetlerinde özellikle bankacılık sektörü gibi; bilgi sistemlerinin yoğun olarak kullanıldığı sektörlerde bilgi sistemleri riskleri ile operasyonel risklerin önemini vurgulamak ve söz konusu risklerin minimize edilmesi amacıyla uygulanması gereken kontrol işlemleri ve bu kontrol işlemlerinin COSO ve COBIT kontrol bileşenleri ile olan ilişkisini açıklamaktır.

Anahtar Kelimeler: Risk, Kontrol, Risk Matrisi, COSO, COBIT, Operasyonel Risk, Bilgi Teknolojileri Riskler, Bireysel Krediler

ABSTRACT

BUILDING RISK MATRIX BY COSO AND COBIT MODELS IN BANKING SECTOR: AN APPLICATION FOR CONSUMER LOAN PROCESS

Developments and changes in the activities and operations have also affected audit scope of control environment of the enterprise and have increased the importance of auditing information systems. In other words, the increase in the use of information technology, even if there is no change in the business processes, has affected the way the activities are conducted, the complexity and control points on the business processes as well as the audit process of these activities.

In the study, the basic and sub-processes carried out in the scope of consumer loan activities in the banks were analyzed and key risks involved in loan operations are defined using by qualitative methods. A risk matrix was established by identifying the control activities that would minimize the identified risks. The main focus is on operational and IT risk in this study and a risk matrix based on COSO and COBIT control models has been create to manage and effectively control of operational and IT risks.

The aim of the study is, to emphasize the importance of information systems risks and operational risks in especially in the banking sector; where information systems are used extensively and to explain the control procedures that should be applied in order to minimize such risks and their relation with COSO and COBIT control components.

Keywords: Risk, Control, Risk Matrix, COSO, COBIT, Operational Risk, IT Risk, Consumer Loans

BANKACILIKTA COSO ve COBIT MODELLERİNE GÖRE RİSK MATRİSİNİN OLUŞTURULMASI: BİREYSEL KREDİLER SÜRECİNE İLİŞKİN BİR UYGULAMA

Sayfa No:

İÇİNDEKİLER…… i
TABLOLAR LİSTESİ…… v
ŞEKİLLER LİSTESİ…….. vi
KISALTMALAR LİSTESİ…… vii
GİRİŞ…… 1

1. BÖLÜM
RİSK VE KONTROL KAVRAMLARINA GENEL BAKIŞ

Sayfa No:

1.1. Risk, Kontrol ve İç Kontrol Kavramları……..…… 6
1.2. Risk Kavramı ve Önemi…..…… 6
1.3. Risk İle İlişkili Olan Kavramlar…..……. …….. 12
1.4. Kontrol ve İç Kontrol Kavramı……..... 14
1.4.1. İç Kontrol Kavramının Amaçları……. 17
1.4.2. İç Kontrol Kavramının Önemini Artıran Gelişmeler……. 23
1.4.3. İç Kontrol Sistemi ile ilgili Düzenlemeler…..…….. 29
1.4.4. Bankacılık Sektöründe İç Kontrol Kavramı..…… 35
1.4.5. Denetim Standartları Kapsamında İç Kontrol Sistemi…….. 36
1.5. COSO ve Kurumsal Risk Yönetimi…….... 39
1.5.1. COSO Kurumsal Risk Yönetimi Bütünleşik Çerçevesi……...39
1.5.2. Anahtar ve Performans Risk Göstergeleri…….……...60

2. BÖLÜM
BANKACILIK SEKTÖRÜNDEKİ RİSK SINIFLAMALARI VE RİSK YÖNETİMİ KAVRAMI

2.1. Bankacılıkta Risk Kavramı…… 65
2.2. Bankaların Sektör Bünyesinde Karşılaştıkları Temel Risk Çeşitleri…… 73
2.3. Bankaların Karşılaştığı Diğer Risk Türleri…… 82
2.4. Bankalarda Bilgi Sistemleri Riskleri…….. 83
2.5. Bilgi Teknolojileri Risk Tanımı ve Operasyonel Risk ile Bağlantısı…… 85
2.5.1. Bilgi Teknolojileri Risk Tanımı…….. 85
2.5.2. Bilgi Teknolojileri Risk Çeşitleri……...88
2.5.3. Bilgi Teknolojileri Risklerinin Operasyonel Riskler ile Bağlantısı…. 91
2.6. Bankalarda Risk Değerlendirme Metodolojisi……97
2.6.1. Risk Belirleme Süreci……..... 97
2.6.2. Risk Değerlendirme Metodolojisi ve Yaklaşımı……..99
2.6.3. Risk Matrisi-Kontrol Kataloğu İçeriğinin Oluşturulması……...102
2.6.4. Risk Değerlendirme Metodolojisinde Kontrol Kataloğunun Rolü….. 106
2.7. Bankalarda Risk Yönetimi……..109
2.7.1. Türk Bankacılık Sektöründe Risk Yönetimi……109
2.7.2. Basel Kriterlerine Göre Risk Yönetimi……....112

3. BÖLÜM
BANKALARDA BİLGİ TEKNOLOJİLERİNE AİT BENİMSENEN KONTROL HEDEFLERİ

3.1. Bankacılık Sektöründe Bilgi Teknolojilerinin Kullanılması ve Önemi…..... 119
3.2. Bilgi Teknolojileri Standartlarının Gelişimi……..... 121
3.3. Temel COBIT Bileşenleri ve Bileşenler Arasındaki Etkileşim..... 130
3.4. COBIT Kontrol Hedefleri……..……..... 138

3.4.1. Genel Kontroller……. 143
3.4.1.1. Planlama ve Organizasyon……. 144
3.4.1.2. Tedarik ve Uygulama……. 146
3.4.1.3. Hizmet Sunumu ve Destek……. 148
3.4.1.4. İzleme ve Değerlendirme...……..151
3.4.2. Uygulama Kontrolleri ve Sınıfları…….…… 152
3.5. COBIT ve COSO Bileşenleri Arasındaki İlişki…….....159
3.6. Bankacılık Sektöründe Bilgi Sistemleri Denetimi İle İlgili Yasal Mevzuat….. 162

4. BÖLÜM
BANKALARDA KREDİLENDİRME SÜRECİ ve KREDİ SÜRECİNDE YER ALAN RİSK ÇEŞİTLERİNİN ÖNLENMESİ

4.1. Bankacılık Sektöründe Kredi ve Kredi Riski Kavramı…… 168
4.1.1. Kredi Tanımı, Unsurları ve Fonksiyonları…… 170
4.1.2. Kredi Riski Tanımı ve Kredi Riski Çeşitleri……. 174
4.1.3. Kredi Türleri…….176
4.1.3.1. Kullanım Amaçlarına Göre Kredi Türleri…… 177
4.1.3.2. Teminatına Göre Kredi Türleri…… 178
4.1.3.3. Vade Bilgisine Göre Kredi Türleri…….. 179
4.1.3.4. Kullanıldığı Yerlere Göre Kredi Türleri…….. 180
4.1.3.5. Kredi Alıcısının Niteliğine Göre Kredi Türleri….. 180
4.1.3.6. Kredinin Niteliğine Göre Kredi Türleri……. 181
4.2. Bankalarda Kredi Süreci ve Yönetimi…… 182

5. BÖLÜM
COBIT VE COSO KONTROL MODELİ KAPSAMINDA BANKALARDAKİ KREDİLER SÜRECİNE AİT RİSK KONTROL KATALOĞUNUN OLUŞTURULMASI

5.1. Uygulamanın Amacı ve Kapsamı …..... 193
5.2. Krediler Sürecine Ait Temel Risk Tanımlamalarının COBIT-COSO Kontrol Hedefleri ile Bağlantısı……...…….. 195
5.2.1. Krediler Süreci İle İlişkili Olan İş Akış Şemaları……....212
5.2.2. Kredi Başvuru, Değerlendirme ve Tahsis Süreci……213
5.2.3. Kredi Kullandırım Süreci……....231
5.2.4. Kredi Döngüsü-Güncelleme, Tahsilat, İzleme ve Kapama Süreci…..243
5.2.5. Kredi Yakın İzleme ve Kanuni Takip Süreci……..255
5.2.6. Kredi Süreci İle İlgili Olan Yetki ve Parametre İşlemleri……...260
5.2.7. Kredi Süreci İçerisindeki İç Kontrol İşlemleri……267
5.2.8. Kredi Süreci İçerisindeki Genel Kontroller……270

SONUÇ……. 271
KAYNAKÇA……275

TABLOLAR LİSTESİ

Sayfa No:

Tablo 1: Operasyonel ve Bilgi Teknolojileri Risklerinin Bağlantısı……..... 96
Tablo 2: Bilgi Teknolojileri Standartlarının Karşılaştırılması……. 127
Tablo 3: COBIT ve COSO Bileşenleri Arasındaki İlişki……. 160

ŞEKİLLER LİSTESİ

Sayfa No:

Şekil 1: Risk Kavramı Bileşenleri 9
Şekil 2: Risk Tanımı 11
Şekil 3 : Risk İle İlişkili Olan Kavramlar 12
Şekil 4 : COSO Kurumsal Risk Yönetimi Küpü 43
Şekil 5: Hedef Risk Hiyerarşisi 45
Şekil 6: COSO Kurumsal Risk Yönetimi Süreci İş Akışı 57
Şekil 7: Anahtar Risk Faktörleri 61
Şekil 8: Risk Yönetimi Süreci 63
Şekil 9: Örnek Risk Modeli 68
Şekil 10: Bankacılıkta Risk Teriminin Kullanım Aşamaları 70
Şekil 11: Bankalarda Net Döviz Pozisyonları 77
Şekil 12: Yönetim Düzeyine Göre Gereksinim Duyulan Bilgi 86
Şekil 13: Bilgi Teknolojileri Riski Öğeleri 91
Şekil 14: Stratejik Uyum Modeli 94
Şekil 15: Risk Değerlendirme Çerçevesi 100
Şekil 16: Risk Değerlendirme Süreci 102
Şekil 17: Geniş Kapsamlı İş Riski Değerleme Metodolojisinin İçerikleri 104
Şekil 18: Türkiye Bankacılık Sektöründe Risk Yönetimi 111
Şekil 19: COBIT Standartlarının Gelişimi 124
Şekil 20: Bilgi Teknolojileri Standartlarının Bileşimi 128
Şekil 21: Bilgi Teknolojileri Standartlarının Kapsam Seviyesi 129
Şekil 22: COBIT Bileşenleri 131
Şekil 23: COBIT Bileşenleri Arasındaki İlişki 133
Şekil 24: Kontrol Tipleri 141
Şekil 25: Kontrol Tiplerinin Kurum İçerisindeki Yeri 142
Şekil 26: COBIT Kontrolleri Arasındaki Bağlantı 158

KISALTMALAR LİSTESİ

a.g.e. : Adı Geçen Eser
a.g.m. : Adı Geçen Makale
AAA : Amerikan Muhasebe Birliği
ABD : Amerika Birleşik Devletleri
AI : Tedarik ve Uygulama
AICPA : Amerikan Sertifikalı Kamu Muhasipleri Enstitüsü
AIRMIC : The Association of Insurance and Risk Managers
APG : Anahtar Performans Göstergesi
ARG : Anahtar Risk Göstergesi
ATM : Automated Teller Machine
BIS : Bank for International Settlements
BTYD : Bilgi Teknolojileri Yönetişim ve Denetim Konferansı
CBRA : Comprehensive Business Risk Assessment
CIO : (Chief Information Officer) Bilgi Sistemleri Grubu Başkanı
COBIT : Control Objectives for Information Technology
COSO : Committee of Sponsoring Organizations
DS : Hizmet Sunumu ve Destek
EFT : Elektronik Fon Transferi
ERM : Enterprise Risk Management
EMKT : Elektronik Menkul Kıymet Transfer Sistemi
eSAC : Electronic System Assurance and Control
FEI : Finans Yöneticileri Enstitüsü
GKGDS : Genel Kabul Görmüş Denetim Standartları
IEE : İç Denetim Enstitüsü
IFAC : Uluslararası Muhasebeciler Federasyonu
IIA : Uluslararası İç Denetçiler Enstitüsü
IMA : Yönetim Muhasebecileri Enstitüsü
INTOSAI : The International Organisation of Supreme Audit Institutions
ISA : International Standards on Auditing

ISACA **:** Information Systems Audit and Control Association Information Systems Audit and Control Association

ISO **:** International Organization for Standardization

ITGI **:** IT Governance Institute IT Governance Institute

ITIL **:** Information Technology Infrastructure Library

İİBF **:** İktisadi İdari Bilimler Fakültesi

İMKB **:** İstanbul Menkul Kıymetler Borsası

KRY **:** Kurumsal Risk Yönetimi

ME **:** İzleme ve Değerlendirme

MK **:** Manuel Kontrol

OGC **:** Office of Government Commerce

OK **:** Otomatik Kontrol

UFRS **:** Uluslararası Finansal Raporlama Standartları

PMBOK **:** The Project Management Body of Knowledge

PO **:** Planlama ve Organizasyon

POS **:** Point of Sale

SEC **:** Securities and Exchange Commission-Amerikan Sermaye Piyasası Kurulu

SysTrust **:** System Trust

TBB **:** Türkiye Bankalar Birliği

TCMB **:** Türkiye Cumhuriyeti Merkez Bankası

TİDE **:** Türkiye İç Denetim Enstitüsü

TMSF **:** Tasarruf Mevduatı Sigorta Fonu

TÜSİAD **:** Türkiye Sanayicileri ve İşadamları Derneği

TTK **:** Türk Ticaret Kanunu

GİRİŞ

Bilgi çağının öneminin bir kat daha arttığı bugünlerde, bilginin önemi ve ulaşılabilirliği önemli ve maliyetli bir hale gelmiştir. İşletmeler bilgiye daha hızlı ve efektif bir şekilde ulaşabilmek ve rekabetin artmış olduğu koşullara, değişimlere daha hızlı ayak uydurabilmek amacıyla yürüttükleri faaliyet sonuçlarını değerlendirebilmek ve değerlendirme sonuçlarını daha çabuk raporlayabilmek amacıyla; gerçekleştirdiği birçok faaliyeti bilgi sistemleri ile birlikte otomatik hale getirmeye başlamıştır. İş süreçlerinde yer alan birçok faaliyetin otomatik hale getirilmesi, işlemlerin yürütülmesinde rol alan sistemlerin kontrol edilmesi ve denetlenmesi ihtiyacını ortaya çıkarmıştır.

İşletmelerde yer alan iş süreçlerinde bilgi sistemlerinin kullanılması, hem sürecin daha efektif, hem de daha hızlı bir şekilde yürütülmesini sağlamaktadır. Bilgi sistemlerinin kullanımının yanında yürütülen faaliyetlere ait tam, doğru ve etkin bir kontrol ortamının oluşturulmaması, işletme bünyesindeki faaliyetlerin hatalı veya yanlış bir şekilde yürütülmesine neden olabilir.

Yürütülen faaliyet ve operasyonlarda ortaya çıkan gelişmeler ve değişiklikler, işletmenin kontrol ortamına ait denetim kapsamını da etkilemiş olup, bilgi sistemleri denetiminin öneminin artmasına neden olmuştur. Diğer bir ifadeyle, işletmenin iş süreçleri kapsamında bir değişiklik olmasa bile bilgi teknolojilerinin kullanımının artması, faaliyetlerin yürütülme şeklini, karmaşıklığını ve iş süreçleri üzerindeki kontrol noktalarını etkilediği gibi bu faaliyetlerin denetim sürecini de etkilemiştir.

İşletmelerde yürütülen faaliyetlerin bilgi teknolojileri aracılığı ile yürütülmesi, işletmeye ait muhasebe ve finansal raporlama süreçlerinde bilgi sistemlerinin kullanımını arttırmıştır. Kullanımın artması muhasebe ve muhasebe işlemlerine ait oluşan finansal raporlamaya ait genel iş akış şemasını ve uygulamasını değiştirmemekle birlikte, operasyonlar sonucunda oluşan finansal bilgilerin işlenmesini, saklanmasını ve aktarılmasını direkt olarak etkilemektedir. Bu durum işletme bünyesinde oluşturulan iç kontrol ortamının yapısını da değiştirmektedir. Bu değişiklikler ve gelişmeler, finansal

denetim kapsamının temelini değiştirmekle birlikte, finansal denetimin bir parçası olan bilgi sistemleri denetim faaliyetlerinin de önemini arttırmıştır. Finansal denetimin nihai amacında ve kapsamında herhangi bir bir değişiklik olmamakla birlikte; işletme bünyesinde bilgi teknolojilerinin kullanımının artması, faaliyetlerin yürütülme şeklini ve iş süreçleri üzerindeki kontrol noktalarını, risk tanımlamalarını etkilediği gibi denetim sürecini ve yürütülen operasyonel işlemleri de etkilemiş bulunmaktadır.

Yukarıdaki belirtilen gelişmeler kapsamında finansal piyasalar içerisinde önemli bir yere sahip olan bankacılık sektörü bünyesinde yer alan birçok faaliyet içerisinde bilgi teknolojilerinin kullanım alanı artış göstermiştir. Teknolojinin gelişmesine bağlı olarak çalışma içerisinde bankacılık sektöründe yer alan faaliyetlere ait iş süreçleri değerlendirilmiş ve bankaların kredi süreçleri içerisinde önemli bir yere sahip olan bireysel krediler sürecine ait işlemlerin incelenmesine karar verilmiştir.

Bankalar açısından bireysel krediler, risklerin dağıtılabilmesi açısından önem arz etmektedir. Bireysel kredilerin ticari kredilerden farkı; daha küçük tutarlarda ve daha fazla müşteri tarafından kullanılmalarıdır. Bu durum bankalar tarafından dikkate alınarak; bünyesinde yer alan kredi portföylerini çeşitlendirmelerine neden olur. Bu çeşitlendirmenin amacı; söz konusu kredilerin kullanılmasını sağlamaktadır. Bankalar portföylerini bireysel kredi çeşitleri ile geniş bir alana dağıtarak, karşı karşıya kalabilecekleri riskleri en aza indirgeyebilirler. Bireysel kredi kullanıcıları ile ticari kredi kullanıcıları değerlendirildiğinde; çeşit olarak bireysel kredi kullanan kullanıcıların; pazarlık gücünün, ticari kredi kullanan kurumlara oranla daha düşüktür. Bu durum; kredi yükümlülüklerini yerine getirmede kişisel itibar faktörüne ait etkinin yüksek olmasına, krediden alınan faiz ve komisyonların nakit girişinin sağlanmasına ve banka kredi portföyünün çapraz satış imkânının bulunmasına bağlı olarak bankalar için bireysel krediler karlı bir alan olmaktadır. Çalışma kapsamında bireysel krediler sürecine ait ana ve alt süreçlerin seçilme nedeni, bireysel krediler süreci içerisindeki ürün çeşitliliğinin ve işlem adedinin fazla olmasından kaynaklanmaktadır. İşlem çeşitliliği ve sayısı fazla olan operasyonlarda hata sayısının ortaya çıkma olasılığı yüksek olabilmektedir.

Bireysel krediler sürecinin örnek olarak seçilmesiyle birlikte; krediler süreci içerisindeki bireysel kredi faaliyetlerine ait ana ve alt süreçler dikkate alınarak, ilgili

süreçlerdeki oluşabilecek olan riskler belirlenmiş ve bu riskleri minimize edecek olan manuel ve/veya otomatik kontrollerin COBIT (Objectives For Information and related Technology) ve COSO kontrol hedefleri ile bağlantısı kurularak, risk matrisinin oluşturulması sağlanmıştır. Bireysel krediler süreci içerisindeki temel, anahtar risk ve kontroller dikkate alınmıştır.

Çalışma kapsamında, bireysel krediler süreci içerisinde COBIT ve COSO kontrol hedeflerinin hangi seviyede bağlantılı olduğu incelenmeye çalışılmıştır. Çalışmada, banka bünyesinde gerçekleştirilen operasyonel faaliyetler içerisinde bilgi teknolojileri kaynaklarının yoğun olarak kullanılması durumunda; operasyonel faaliyetlere bağlı olarak gerçekleşmesi muhtemel risklere ait oluşturulan kontrollere temel oluşturan COBIT ve COSO kriterlerinin bağlantı düzeyi incelenmiştir.

Çalışmanın amacı, bağımsız denetim faaliyetlerinde özellikle bankacılık sektörü gibi; bilgi sistemlerinin yoğun olarak kullanıldığı sektörlerde bilgi sistemleri riskleri ile operasyonel risklerin önemini vurgulamak ve söz konusu risklerin minimize edilmesi amacıyla uygulanması gereken kontrol işlemleri ve bu kontrol işlemlerinin COSO ve COBIT bileşenleri ile olan ilişkisini açıklamaktır.

Mevcut durumda uygulamanın ana problemi, bankacılık sektöründe faaliyet gösteren bankaların süreçlere ait risk matrisleri ve kontrol katalogları oluşturulmuş olmasına rağmen; ilgili risk matrisleri ve kontrol katalogları; COSO ve COBIT bileşenleri açısından değerlendirilmemektedir. Bankacılık sektöründe süreçlerin etkin bir şekilde test edilmesi amacıyla süreçlere ait oluşturulan risk haritasının, COSO ve COBIT bileşenleri ile ilişkileri kurularak oluşturulması sağlanmalıdır. Çalışma bu yönden teknoloji ağırlıklı olarak çalışan bankalar için referans bir kaynak oluşturmakla birlikte, bireysel krediler süreci içerisindeki temel süreçler örnek olarak seçilerek, banka bünyesinde yürütülen diğer süreçlerin de bu açıdan değerlendirilerek, oluşturulan çalışmanın bir örneğinin diğer süreçler içinde yapılması gerektiğini ortaya koymaktadır.

Bankalarda bireysel kredi faaliyetleri kapsamında yürütülen süreçlerin ve alt süreçlerin değerlendirilmesi, operasyonlarda yer alan anahtar risklerin kalitatif yöntem kullanarak tanımlanması (değerlendirilmesi) ve söz konusu riskleri minimize edecek olan

kontrol faaliyetleri tanımlanarak, ilgili faaliyetlerin COSO ve COBIT kontrol standartları ile olan bağlantısı kurulmaya çalışılmıştır. Çalışma kapsamında bireysel krediler sürecinde yer alan anahtar (temel) risk faktörlerinin test edilmesi amacıyla hangi test işlemlerinin denetim kapsamında uygulanması gerektiğini ortaya koymaktır.

Çalışma içerisinde operasyonel risklerin bilgi teknolojileri riskleri ile olan ilişkileri COBIT ve COSO standartları temel alınarak, beş bölüm içerisinde açıklanmıştır.

Çalışmanın birinci bölümde işletmelerde özellikle bankacılık sektöründe yoğunluklu olarak kullanılan risk, kontrol ve iç kontrol kavramları teorik olarak açıklanmıştır. Çalışma içerisinde iç kontrol kavramının amaçlarına yer verilmiş olup, iç kontrol kavramının önemini arttıran gelişmelere ve olaylara yer verilmiştir. Dünyada ve Türkiye'de iç kontrol sistemi ile ilgili olarak gerçekleştirilen düzenlemeler açıklanmış olup, düzenlemelerden en önemlisi olan COSO yapısına, kurumsal risk çerçevesi kapsamında yer verilmiştir. İlgili bölüm içerisinde COSO uygulaması dışında genel kabul görmüş olan diğer iç kontrol yapılandırmaları (COBIT, eSAC, SysTrust) tanımlanmıştır. COSO bileşenleri ve bileşenlerin birbirleri ile olan ilişkileri ayrıntılı olarak birinci bölüm içerisinde açıklanmış, anahtar performans göstergesi ve anahtar risk göstergesi kavramlarına özet olarak değinilmiştir.

İkinci bölüm içerisinde diğer sektörlerde faaliyet gösteren işletmelerin karşılaştıkları ortak risk çeşitleri ve bankacılık sektörü bünyesinde karşılaşılan risk çeşitlerine yer verilmiştir. Bölüm içerisinde bilgi teknolojileri kapsamındaki risk tanımlaması yapılmıştır. Bilgi teknolojileri kapsamında risk çeşitlerine yer verilmiş olup, bilgi teknolojileri risklerinin operasyonel riskler ile olan bağlantıları açıklanmıştır.

Bankalarda teknolojinin yoğun olarak kullanılmasına bağlı olarak karşılaşılan risk çeşitleri içerisinde yer alan bilgi sistemleri risklerine değinilmiştir. Bölüm içerisinde bankacılık sektöründeki risk değerlendirme metodolojisine yer verilerek, risk matrisi kavramlarına yer verilmiştir. Bölüm başlıklarında Basel kriterlerindeki ve Türk Bankacılık sektöründeki risk yönetiminin içeriğine yer verilmiştir.

Üçüncü bölümde; bilgi teknolojilerine ait risk çeşitleri ile ilgili tanımlamalar yapıldıktan sonra; bankaların maruz kaldıkları bilgi teknolojileri risklerinden

etkilenmemek amacıyla bankacılık sektöründe kullanılan ve benimsenen COBIT kontrol hedefleri açıklanmıştır. COBIT kontrol hedeflerine bağlı olarak, bilgi teknolojileri kontrol standartlarının tarihsel gelişimleri ve COBIT uygulaması ile arasındaki farklar açıklanmıştır. Bölüm içerisinde COBIT standardında yer alan **"uygulama"** ve **"genel"** kontrol tanımlamalarına detaylı olarak yer verilmiştir. COSO ve COBIT bileşenleri arasındaki ilişki açıklanarak, bankacılık sektöründe bilgi sistemleri denetimi ile ilgili olarak uygulanan yasal mevzuat bilgilerine yer verilmiştir.

Dördüncü bölüm içerisinde, bankaların operasyonel olarak gerçekleştirdiği temel süreçlere yer verilmiş olup, belirtilen bu süreçler içerisinde yer alan bireysel ve kurumsal krediler süreçleri ile direkt bağlantısı olan kredi ve kredi riski tanımlamaları yapılmıştır. Kredi kavramı, çeşitleri, unsurları ve fonksiyonları bu bölüm içerisinde açıklanmaya çalışılmıştır. Bankalarda gerçekleştirilen kredi işlemlerine ait süreç bilgilerine ve kredi yönetimi kavramına yer verilmiştir.

Beşinci bölüm içerisinde ağırlıklı olarak uygulama çalışmasına yer verilmiştir. Banka bünyesinde standart bir kredilendirme süreci kapsamında yer alan temel ve alt süreçler tanımlanmış olup, söz konusu süreçlere ait iş hedefleri belirlenmiştir. İş hedeflerine ait karşılaşılabilecek risk tanımlamaları ortaya konulmuş olup, risk tanımlamalarına ait kontroller belirtilmiştir. Süreç ve alt süreç kapsamındaki kontroller, COSO ve COBIT kontrolleri kapsamında değerlendirilerek, kontrollerin COSO ve COBIT kontrol hedefleri ile ilişkisi gösterilmiştir.

COBIT ve COSO kontrol hedeflerinin birlikte kullanılması durumunda, bankacılık sektörüne ait kredi süreci içerisindeki hangi standart riskleri minimize edebileceği açıklanmıştır.

Bölüm içerisinde bankalarda yürütülen bireysel kredi işlemlerine ait süreç ve alt süreçler yer verilmiş, temel risk ve kontrol tanımlamaları yapılmış olup, söz konusu kontrol türleri COSO ve COBIT bileşenleri ile ilişkilendirilmiştir.

1. BÖLÜM
RİSK VE KONTROL KAVRAMLARINA GENEL BAKIŞ

1.1 Risk, Kontrol ve İç Kontrol Kavramları

Çalışmanın bu bölümünde, bankacılık sektöründe yer alan faaliyetler içerisinde yoğun olarak kullanılan olan risk, kontrol ve iç kontrol kavramları açıklanmıştır. Bölüm kapsamında ilgili kavramların birbirleri ile olan bağlantılarına COSO kurumsal yönetim çerçevesinde yer verilmiştir. Bu kavramlar çalışma içerisinde öncelikli olarak teorik olarak tanımlanmış olup, bankacılık sektöründe krediler sürecinde operasyonel açıdan ortaya çıkan risklerin ve kontrollerin anlaşılması açısından büyük önem taşıyacaktır.

1.2 Risk Kavramı ve Önemi

Günümüzde bütün işletmelerin bir kuruluş amacı bulunmaktadır. İşletmelerin kuruluş amacına ulaşabilmek için işletme bünyesinde oluşturulan organizasyon çerçevesinde, bünyesinde kapsam ve içeriğine göre birçok faaliyet gerçekleştirilir. Gerçekleştirilen faaliyetler bir hedefe yönelik oluşturulmakla birlikte, söz konusu belirlenen hedefler işletmenin üst yönetimi tarafından karara bağlanır. Karara bağlanan hedeflere ulaşabilmek için işletmeler risk ve/veya risklerle karşılaşabilir.

Risk, her alanda bireyleri, işletmeleri, toplumu yakından ilgilendiren, yaşamın ayrılmaz bir parçası ve önemli bir unsurudur. Risk kavramı, güncel hayat içerisinde çok fazla kullanılmakla birlikte; riskin tanımlamasını yapmak oldukça zor bir konu olarak karşımıza çıkmaktadır. Risk, belirsizlik ve/veya belirsizliğin bir sonucu olarak tanımlanabilir. Risk; belirli bir zaman aralığında, hedeflenen bir sonuca ulaşmada, kayba ya da zarara uğrama olasılığı veya bir olayın sonucunun tam olarak gerçekleşebilme olanağıdır.[1] Risk kelime anlamı olarak "bir tehlikeyi, kaybı ve/veya zararı ortaya

[1] Mustafa BAŞARIR, "Bankalarda Teknoloji Riski ve Yönetimi", **Yüksek Lisans Tezi**, İstanbul: Marmara Üniversitesi, Bankacılık ve Sigortacılık Enstitüsü, 2006, s.3.

çıkartabilecek bir durumun oluşması ve ortaya çıkma olasılığıdır." Kelime anlamı olarak "tehlike" anlamını ifade eder.

Risk, her işletmede karşılaşılan bir kavram olup, işletmelerin ayrılmaz bir parçasıdır. İşletme bünyesinde yer alan ve her an ortaya çıkmaya hazır olan riskler, işletme bünyesindeki organizasyon içerisinde tam, doğru ve zamanında tespit edilip, yönetilmemesi durumunda, işletmenin hedeflerine en kısa sürede ve verimli bir şekilde ulaşabilme, rekabet, finansal durum, performans ve kurumsal itibar gibi fonksiyonları üzerinde olumsuz yönde etki edebilir. Bu olumsuz etkilenme, hem işletmeyi hem de işletme bünyesindeki tüm paydaşlara yansıyabilmektedir. İşletmeler faaliyetlerini yürütürken risksiz bir ortamda faaliyette bulunamayacağı gibi, karşılaşılan risklerin başarılı bir şekilde yönetilmesi gerekliliğini ortaya çıkartmaktadır.[2]

Risk; işletme amaçlarını olumsuz etkileyebilecek olayların gerçekleşme olasılığını ifade eder.[3]

Günümüzde, geçmişte ve gelecekte karşılaşılan riskleri azaltma ve yönetme çabası, önem olarak hiçbir şey kaybetmemektedir. Özellikle finans sektörü için önemi gittikçe de artmaktadır. Son zamanlarda yaşanan finansal krizler finans sektörü için risk kavramının artık hayati bir önem kazanmasını sağlamıştır. Geçen süre kapsamında meydana gelen faaliyetlerde ortaya çıkan büyük değişimle birlikte, işlem çeşitliliği, hacmi ve hızı artmış olup; risk çeşitlerini, boyutlarını ve risklerle karşılaşma sıklığını ve olasılığını da artırmıştır. Risklerin farkında olmayan ve gösterilmesi gereken özeni göstermeyen işletmeler, bünyesinde kayıplar yaşamış ve büyük risklere maruz kalmıştır. Bu durumları yaşayan işletmeler çok zor durumda kalarak bu riskleri minimize etmiş veya bu risklerin üstesinden gelememiştir. Bu işlemlerin sonucu olarak operasyonel faaliyetlerini sona erdirmek zorunda kalmışlardır. Bu nedenle, günümüzde finansal sektörde yer alan işletmeler, stratejik kararlar alırken ve bu alınan kararların

---

[2] Nejat BOZKURT, Cemal İBİŞ ve Çağla AKDEMİR, "6102 Sayılı Türk Ticaret Kanunu Kapsamında Bağımsız Denetim ve Hile Riski", **Dış Denetim Dergisi**, Ekim-Kasım-Aralık 2011, s.168.

[3] Işılda ARSLAN, "Kurumsal Risk Yönetimi", Maliye Bakanlığı Strateji Geliştirme Başkanlığı, 2008, s.8.

değerlendirilmesini yaparken, ihtiyaç duydukları ölçütlerin başında "risk" faktörünü göz önüne almaya başlamışlardır.

Finansal kurumlar açısından risk en genel anlamda; "İstenmeyen durumlarla karşılaşma olasılığıdır."[4] Finans kuramı çerçevesinde risk genel olarak, finansal işlemlerin ileride veya mevcut durumda sağlayacağı getiri ile bu işlemlerle ilgili nakit akışlarının beklenen bugünkü değeri arasındaki fark olarak tanımlanmaktadır. Teknik anlamda riskin tanımı, "Getirilere ilişkin olasılık değerlerinin ortalama değer etrafındaki dağılımını ifade eder".[5] Bu bakımdan söz konusu olasılık dağılımını etkileyen her şey, yatırım riskini de olumlu ve olumsuz olarak çift yönlü olarak etkileyecektir.

Riskin tanımı; belirsizlik, tehlike ve fırsat kavramları olarak ayrı olarak tanımlanmaktadır. Bu tanımlamalar dikkate alındığında risk[6];

- Planlanan amaçlardan sapmayı ortaya çıkaran her türlü durum bir risktir. Risk, gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eder.

- Risk, tehlike ve belirsizliği kapsamaktadır; ancak tehlike ve belirsizlikler arayışları ortaya çıkardığından dolayı, fırsatları da barındıran çok önemli bir faktördür.

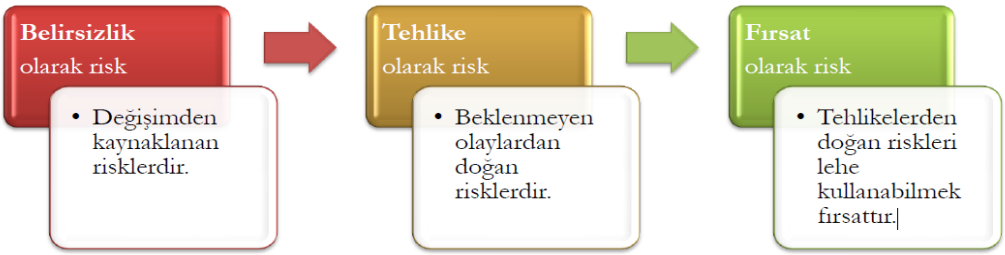
- Beklenmeyen olaylardan kaynaklanan risk tehlikeyi, değişimlerden kaynaklanan risk belirsizliği, çeşitli tehlikeleri işletmenin lehine kullanabilme yeteneği de fırsatları beraberinde getirmektedir.

---

4 İMKB, "Sermaye Piyasası ve Borsa Temel Bilgiler Kılavuzu", İstanbul, 1999, s.476.

5 Serdar ÇITAK, "Geleneksel Risk Yönetiminden Programlanmış Menkul Kıymet İşlemlerine, Ekonomi Dizisi:7", **Dünya Yayınları**, İstanbul, Ekim 1999, s.11.

6 Sezer Bozkuş KAHYAOĞLU, "Kurumsal Risk Yönetimi Standartları-Yeni Türk Ticaret Kanunu Çerçevesinde Türkiye Uygulaması", 2012, http://www.gtturkey.com/ud_objs/pdf/etknlk/musiad_risk_yonetimi_sunumu.pdf, (09.05.2014), s.6.



Şekil 1: Risk Kavramı Bileşenleri
Kaynak: Sezer Bozkuş KAHYAOĞLU, "Kurumsal Risk Yönetimi Standartları-Yeni Türk Ticaret Kanunu Çerçevesinde Türkiye Uygulaması", 2012 http://www.gtturkey.com/ud_objs/pdf/etknlk/musiad_risk_yonetimi_sunumu.pdf, (09.05.2014), s.6.

Günümüzde çoğu kez **risk** ve **belirsizlik** kelimeleri anlam olarak birlikte kullanılmaktadır. Ancak anlam bütünlüğü açısından bakıldığında; bu iki kavramın birbirinden farklı bir şekilde kullanılması gerektiği ortaya çıkmıştır.

Belirsizlik, bilgisizlik ve geleceğin taşıdığı olası sürprizleri, risk ise tehlike ve korunmasızlık anlamları içinde yer alır.[7] Bu bakımdan, her iki tanımlamayı ayırmak amacıyla şu şekilde ayırıcı bir tanımlama yapılabilir. "Risk, bilinen ya da beklenen bir tehlikeye açıklık oranında kayba uğrama olasılığıdır." Tehlikenin varlığı ve boyutu tam olarak bilinmiyorsa belirsizlik riski, tehlikeye açıklık ve korunmasızlık tam olarak bilinmiyorsa risk belirsizliği içinde taşır. [8]

Belirsizlik kavramının finansal olarak anlamı, "elde edilecek olası sonuçların dağılımı" olarak tanımlanabilir. Bu bakımdan risk gerçekleşmesi en muhtemel sonuç (beklenen) ile fiili (gerçekleşen) sonuç arasındaki sapmadır. Söz konusu dağılım ne kadar geniş ise belirsizliğinde o kadar fazla olacağı kabul edilebilir.

---

[7] Timuçin YALÇINKAYA, "Risk ve Belirsizlik Algılamasının İktisadi Davranışlara Yansımaları", **Muğla Üniversitesi İİBF Tartışma Tebliğleri**, No:2004/05, 2004, s.7.

[8] Aytekin GÜVEN, "Yatırımlar, Belirsizlik ve Piyasa Yapısı: Kavramsal Bir İnceleme", **Afyon Kocatepe Üniversitesi İBBF Dergisi**, Cilt:15, Sayı:1, 2013, s.17.

Bu açıklamalardan sonra belirsizlik tanımı daha açık ve net bir şekilde ortaya çıkmaktadır. Belirsizlik, beklenen sonuçlara ilişkin olasılık değerlerinin tahmin edilememesi veya saptanamaması durumudur.[9]

Tanımlamalardan da anlaşılacağı gibi, finansal anlam olarak çoğunlukla eşanlamlı olarak kullanılan belirsizlik tanımlaması, riskten daha genel bir anlam taşımaktadır. İşletmelere problem yaratabilecek olan risk kavramı değil, belirsizlik kavramıdır. Bunun nedeni, finansal piyasalarda risk ölçülebilen ve yönetilebilen bir durum olarak ortaya çıkarken, belirsizlik kavramı için aynı durum söz konusu değildir.

Riskin iki temel özelliği bulunmaktadır. Bunlar **olasılık ve etki** kavramlarından oluşmaktadır.[10]

Olasılık: Hedeflenen amaca/amaçlara ulaşamama olasılığı ya da istenmeyen bir olayın oluşma olasılığını ifade eder.

Etki: Risk olan durumun oluşması sonucu hedeflenen amaç(lar)dan ortaya çıkan sapmalar, riskin büyüklüğünü ve şiddetini gösteren etkisidir.

ISO (International Organization for Standardization) /IEC 73. prensibine göre risk, bir faaliyete ait birleştirilmiş olasılıkları ve sonuçları ifade eder. Her çeşit bütün girişimlerde, potansiyel işlemler ve sonuçlar; başarıya ulaşabilmek amacıyla fayda veya tehdit için fırsatlar sunmaktadır. Risk yönetimi, riskin her iki yönü olan pozitif ve negatif etkileriyle gün geçtikçe daha fazla ilgilenmeye başlamıştır. Risk yönetimi kavramı son yıllarda hızlı bir şekilde disiplinler geliştirmiştir. Günümüzde risk yönetiminin ne olduğu ve ne işe yaradığı hakkında çeşitli incelemeler ve tanımlamalar yer almaktadır. Risk yönetimi sadece işletmeler veya kamusal organizasyonlar için değildir ancak faaliyetlerin uzun veya kısa dönemde gerçekleşip gerçekleşmemesi açısından kurumlar için önemli bir hal almaktadır.

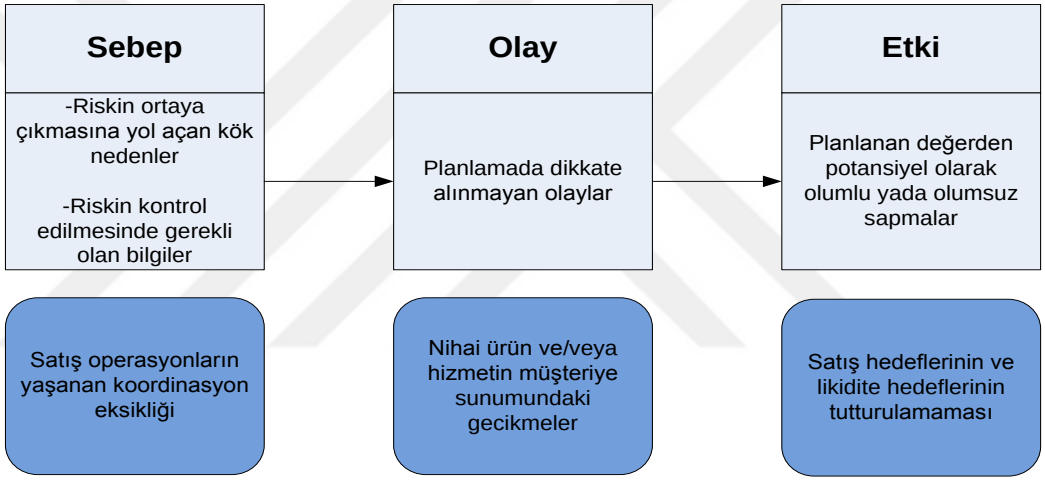
---

[9] J.F. WESTON ve F.E. BRIGHAM, **Managerial Finance**, Dryden Press:5th Ed., London, 1975, s.313.

[10] KAHYAOĞLU, a.g.e., s.8.

Riskin kavramsal olarak tarihi gelişimi değerlendirildiğinde; risk geçmiş dönemlerde bir tehdit olarak algılanmakta, daha sonraki dönemlerde temel araç olarak işletmenin kendi kendini değerlendirmesi olarak algılanmaya başlanmıştır. Günümüzde ise risk kavramı fırsat olarak değerlendirilmektedir. Risk kavramını günümüzde stratejik, ileriye dönük ve proaktif sürekli izlenebilen bir kavram olarak dikkate alınmaktadır.

Risk kavramsal olarak, olumsuz bir olayın-durumun meydana gelme olasılığı olarak tanımlanmakla birlikte, diğer bir yaklaşımla birlikte işletmelerin hedeflerine ulaşmasında olumlu ve/veya olumsuz bir yönde etki eden bir olayın-durumun meydana gelme olasılığını ifade etmektedir.

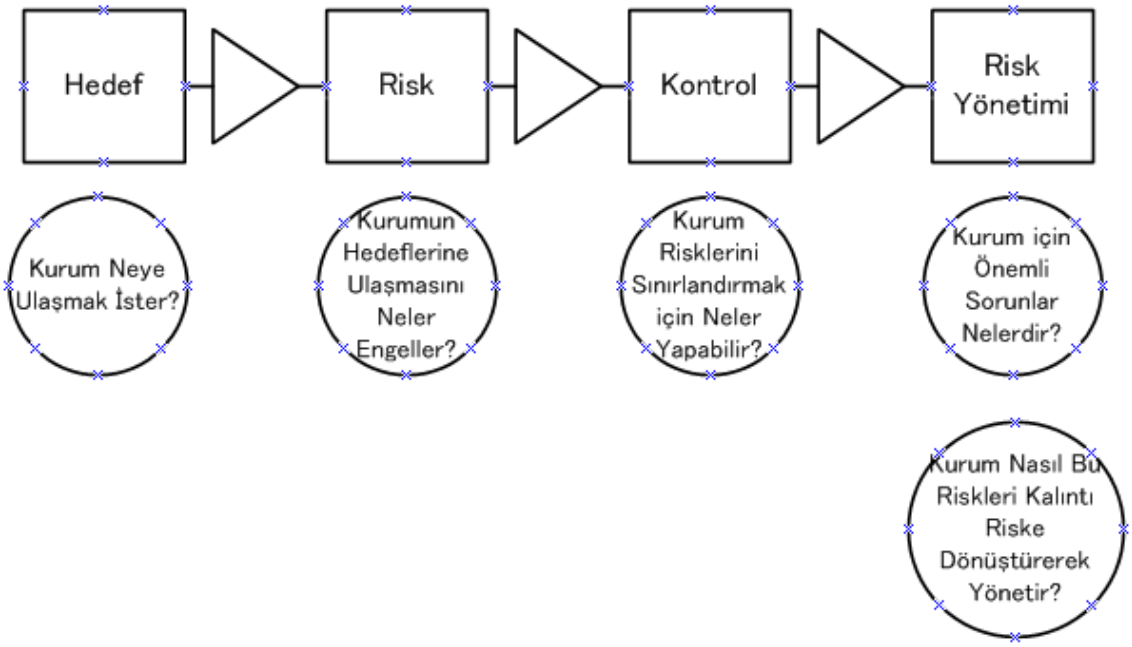


Şekil 2: Risk Tanımı
Kaynak: Sezer Bozkuş KAHYAOĞLU, "Kurumsal Risk Yönetimi", **KPMG Gündem Dergisi**, Sayı: 9, Ocak-Mart 2012, s.42.

Sebep, olay ve etki kavramları birlikte değerlendirilerek risk tanımlaması yapılmalıdır. İşletme içerisinde kritik görevlerde rol alan bölümlerin işletme bünyesinde oluşan ve/veya oluşması beklenen risklere ait risk tanımlaması yaparken, söz konusu risklere neden olan **ana nedenlerin** ve/veya çıkabilmesine neden olacak olan ve **planlamada dikkate alınmayan operasyonların-faaliyetlerin gözden geçirilmesi, tam, doğru ve zamanında incelenmesi** gereklidir. Riske neden olan ana sebeplerin belirlenmesi, risklerin kontrol edilmesinde kullanılacak olan en önemli bilgileri içerir. Bu bilgiler değerlendirilip, gözden geçirildikten sonra risk tanımlaması tamamlanarak, yapılan tanımlamaların işletme bünyesindeki etkileri belirlenir.

1.3 Risk İle İlişkili Olan Kavramlar

Risk tanımlaması kapsamında risk kavramının ilişkili olduğu kavramlar; **hedef, kontrol ve risk yönetimi** olarak karşımıza çıkar. İşletmenin bünyesinde yer alan faaliyetlerin sürdürebilir bir şekilde yürütülebilmesi, söz konusu bu kavramların birbirleri ile olan bağlantısına ve ilişkisine bağlı olmaktadır.



Şekil 3 : Risk İle İlişkili Olan Kavramlar

Hedef: İşletme bünyesinde tanımlanan hedefler dikkate alındığında, hedef belirlerken iki temel kavramın dikkate alınması gereklidir. Bu kavramlar, **genel işletme stratejileri ve işletmenin risk alma** profilidir. İşletme bünyesinde kurumsal risk alma durumunun ortak bir anlayışta olması gereklidir. Bu durum, işletmenin bünyesinde genel mevcut konumunu, hedeflerini ve bu hedeflerine nasıl ulaşacağını tanımlayan bir işletme stratejisi ve politikası ile oluşturulabilir. İşletme stratejisi ve politikası oluşturulmadan işletmenin kurumsal risk alma profilinin uygunluğu değerlendirilememektedir. İşletme stratejileri ve kurumsal risk alma potansiyelleri birbirlerini tamamlayan ve etkileyen kavramlar olmakla birlikte her iki kavram için biri diğerinin sonucu olarak algılanmamalıdır. İşletme bünyesinde uygulanan bu kavramların birbirleri ile uyumlu olması ve koordineli bir şekilde uygulanması sağlanmalıdır. İşletme içerisinde yer alan

organizasyonel yapı içerisinde, işletme hedefleri ve stratejileri belirlenerek ortaya konulmalıdır. İşletme hedef ve stratejilerinin belirlenmesi; işletme bünyesinde risk yönetimi uygulamalarına ana bir yapı oluşturmakla birlikte, işletmeye değer yaratılması sağlanarak, uygun ve ideal bir iş modelinin işletme bünyesinde tanımlanmasına neden olacaktır.[11]

Risk: Risk, "bir kurumun, hedeflerini elde etmek ve değer katmak için anladığı ve yönettiği belirsizlikler" olarak tanımlanmaktadır. Tanımlamanın kapsamı, işletmenin organizasyon seviyelerini bütünüyle ayrıntılı bir şekilde kapsamakta olup; risk yönetim kavramı, işletmenin bütün seviyelerinde bulunan yönetimin sorumlu olduğunu ifade eder. İşletmenin sahibi olan paydaşlar tarafından, işletme faaliyetleri içerisinde karşılaştığı bütün riskleri işletme stratejileri ve hedefleri doğrultusunda uygun bir şekilde yöneteceğini genel olarak kabul eder.

Kontrol: Kontrol, işletme yönetiminin, denetim kurulunun, yönetim kurulunun ve işletme bünyesinde yer alan diğer uygun birimlerin riski yönetmek ve belirlenen amaç ve hedeflere ulaşma olasılığını arttırmak amacıyla aldığı tedbirlerdir. Yönetim, hedef ve amaçların gerçekleştirilmesine yönelik makul bir güvence sağlamak için yeterli tedbirin alınmasını planlar, tertipler ve yönlendirir.[12]

Risk Yönetimi: İşletme amaçlarını gerçekleştirmek üzere makul bir güvence sağlamak amacıyla potansiyel olay ve durumları belirlemesi, değerlendirmesi, yönetmesi ve kontrol edilmesi sürecidir.[13]

---

11 TÜSİAD, "Kurumsal Risk Yönetimi", **Kurumsal Risk Yönetimi Grubu Çalışması**, Aralık 2006, s.23.

12 The Institute Of Internal Auditors (IIA), **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi**, Red Book, TİDE, Lebib Yalkın Yayımları, s.5.

13 The Institute Of Internal Auditors (IIA), a.g.e., s.6.

1.4 Kontrol ve İç Kontrol Kavramı

Kontrol kavramının içeriği incelendiğinde kontrol faaliyeti; planlanan bir amaca ulaşılıp ulaşılmadığının değerlendirilmesi ve araştırılması faaliyetidir.[14] Kontrol işletme yönetiminin en kritik ve en önemli fonksiyonlarından biri olup; işletmenin bulunduğu sektördeki faaliyet sonuçlarını tespit ederek, diğer işletme fonksiyonlarının işletme hedeflerine bağlı olarak başarısını ölçerek işletme yönetimine ışık tutar. Kontrol, bir işletmenin amaçlarına en verimli şekilde ulaşmasını sağlayan önlemlerdir.[15] Kontrol işletmenin bütün faaliyet ve fonksiyonlarını kapsayarak, işletme bünyesinde oluşan hataları ortaya çıkararak; hataların tekrar ortaya çıkmasını engellemek amacıyla işletmeye ait faaliyetlerdeki hata noktalarını ve noksanlarını tespit etmeyi amaçlamaktadır.[16]

İç Denetim Enstitüsü (IIE) kontrolü şu şekilde tanımlamıştır;

"Kontrol, yönetimin, denetim kurulunun, yönetim kurulunun ve diğer uygun birimlerin riski yönetmek ve belirlenen amaç ve hedeflere ulaşma ihtimalini artırmak amacıyla aldığı tedbirlerdir. Yönetim, hedef ve amaçların gerçekleştirilmesine yönelik makul bir güvence sağlamak için yeterli tedbirin alınmasını planlar, tertipler ve yönlendirir." [17]

İşletme bünyesinde yer alan kontrol türleri yürütülen faaliyetin önemine ve çeşidine göre tasarlanır. İşletme bünyesinde yürütülen faaliyetlere ait istenmeyen

---

[14] Türkiye Bankalar Birliği, "Bankalarda İç Denetim ve Bankacılık Gözetim Otoritesinin İç ve Dış Denetçiler İle İlişkisi", **Bankacılık Gözetimine İlişkin Basel Komitesi Tarafından Yayımlanan Danışma Belgesi**, Temmuz 2000, s.8-9.

[15] Şaban UZAY, "İşletmelerde İç Kontrol Sistemini İncelemenin Bağımsız Dış denetim Karar Sürecindeki Yeri ve Türkiye'deki Denetim Firmalarına Yönelik Bir Araştırma", **Sermaye Piyasası Kurulu**, Yayın No:132, Ankara, 1999, s.5.

[16] Cemal ELİTAŞ, "Kontrol Önlem ve Yordamlarının İç Denetçi Açısından Rolü ve Önemi", **İç Denetim Dergisi**, Sayı:8, 2004, s.34.

[17] İç Denetim Enstitüsü, "Terimler Sözlüğü: Kontrol (Control)", http://www.tide.org.tr/page.aspx?nm=terimler_sozlugu, (08.09.2010), s.2.

sonuçların önlenmesi için kontroller tasarlanmış ise bu tip kontrollere **önleyici kontroller** denir.[18]

İşletme bünyesinde tasarlanan kontroller, faaliyetlere ait riskler gerçekleştiklerinde istenmeyen sonuçları tanımlamak için tasarlanmış ise bu çeşit kontroller **(belirleyici) tespit edici** kontroller olarak tanımlanır.

İşletme bünyesinde tasarlanan kontroller işletme tarafından kabul edilmeyen faaliyet sonuçlarını tersine çevirmek veya tekrar ortaya çıkmalarını önlemek için düzeltici bir eylemin yapılmasının sağlanması amacıyla tasarlanan kontroller ise **düzeltici kontroller** olarak tanımlanır.[19]

Kavram olarak kontrol ve denetim tanımlamaları uygulama anlamında birden fazla sefer aynı zamanda düşünülmekte ve söylenmektedir. Kavramlar daha dikkatli ve ayrıntılı olarak değerlendirildiğinde; kontrol fonksiyonun denetimden daha geniş ve öncelikli olarak öne çıktığı görülmektedir. Bunun nedeni, kontrol işleminin faaliyetlerin ve operasyonların aktive edildiği zaman yapılmasıdır. Kontrol işlemi anlık olarak gerçekleştirilmekte olup, ilgili zaman dilimi içerisinde gerçekleştirilen faaliyetleri ve faaliyet sonuçlarını dikkate alır. Denetim faaliyeti ise geçmiş bir zaman dilimindeki işlemleri değerlendirir ve sonuçları ile ilgilenir. Kontrol işlemi işletme sistemi içerisinde gerçekleştirilen faaliyet kapsamında görev alan işletme personeli tarafından yapılmakta ve koordine edilmekte olup, denetim işlemi operasyonel faaliyetten bağımsız olan uzman kişiler tarafından gerçekleştirilir. Denetim ve kontrol faaliyeti ilişkili kavramlar olup, kontrolün etkililiği ve efektifliği denetim kapsamının etkililiğine olumlu yönde katkı yapar.[20]

"Kontrol" birinci isim olarak bir unsuru veya öğeyi ifade eder. Örneğin; işletme bünyesindeki iç kontrol sisteminin bir parçası olan politika ve prosedürler, kontrol

---

18 Özgür ÇATIKKAŞ, "Bankalarda İç Kontrol Sistemi ve İç Denetim Fonksiyonunun Etkililiği", **Doktora Tezi**, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü Bankacılık Anabilim Dalı, İstanbul, 2005, s.4.

19 ÇATIKKAŞ, a.g.e., s.4.

20 Çiğdem SOLAŞ, "Bankalarda İç Denetim Tekniği ve Türk Uygulaması", **(Yayınlanmamış Doçentlik Tezi)**, Marmara Üniversitesi, İstanbul, 1975, s.55.

faaliyetinin varlık sebebini oluşturur. **"Kontrol"** kavramı ikinci isim olarak bir konumu veya şartı-kriteri ifade eder. Örneğin, işletme bünyesinde oluşturulan politika ve prosedürlere ait ortaya çıkan sonuçlar, işletme bünyesindeki iç kontrolün etkinliğini etkiler. Kontrol, üçüncü olarak **"eylem-faaliyet"** kavramı olarak kullanılır. Örnek olarak, işletme bünyesinde kontrolleri etkileyen politikaların oluşturulması veya yürütülmesine yönelik olarak imkânların oluşturulmasıdır.[21]

İşletme yönetimi kapsamında kontrol kavramı, yönetimin beş temel fonksiyonundan biri olup, işletmenin (tedarik, üretim, pazarlama, personel, muhasebe ve finansman, halkla ilişkiler vb.) tüm fonksiyonlarını ve faaliyetlerini kapsayarak, işletme bünyesinin bütününde yer alır. Yönetimin beş temel fonksiyonu aşağıdaki gibidir:[22]

1. Planlama,
2. Örgütleme,
3. Yürütme,
4. Koordinasyon,
5. Kontrol,

Başlangıç fonksiyonu planlama ve örgütlenme ile başlamakla birlikte bu fonksiyon teknik özellikleri ve deneyim kavramını içerir. Tedarik işlemlerinden müşterilerle ilişkilere kadar işletmeye ait bütün faaliyetlerin planlanması, organize edilmesi, planlı bir şekilde faaliyete geçirilmesi gereklidir. Faaliyetlerin ve faaliyet sonuçlarının mutlak suretle işletme bünyesinde kontrol edilmesi sağlanmalıdır.

---

21 ARSLAN, a.g.e., s.6.

22 Cemal İBİŞ ve Özgür ÇATIKKAŞ, "İşletmelerde İç Kontrol Sistemi'ne Genel Bakış", **Sayıştay Dergisi**, Sayı:85, Nisan-Haziran 2012, s.97.

1.4.1 İç Kontrol Kavramının Amaçları

İç kontrol, işletmenin, yönetim kurulu, üst düzey yönetimi ve tüm çalışanları tarafından yönlendirilen, gerçekleştirilen, işletme tarafından belirlenmiş konularda hedeflerin başarılması açısından makul bir güvence sağlamak üzere tasarlanmış bir süreçtir. Bu sürecin amaçları,[23]

- Faaliyetlerin etkinliği ve verimliliği,
- Mali raporlama sisteminin güvenilirliği,
- Mevzuata uyumu sağlamaktır.

Yukarıdaki belirtilen amaçlar kapsamında iç kontrol kavramı aşağıdaki belirtilen konuları işletmeye sağlar;[24]

- İşletme bünyesinde yürütülen işlemlerin yönetimin belirlediği hedefler ve stratejiler kapsamında etkinliğinin ve verimliliğinin artmasını sağlar:
  - ✓ Süreçlerin standartlaşmasını sağlayarak, faaliyetlerin ekonomikliğini, verimliliğini ve etkinliğini artırır.
  - ✓ İşletme bünyesinde yer alan varlıkların kontrol faaliyetleri aracılığıyla korunmasını sağlar.
- İşletme tarafından yürütülen faaliyet sonuçlarına ait mali ve/veya mali olmayan raporlama sisteminin güvenilirliğini sağlar:
  - ✓ İşletme stratejilerinin yenilenmesi, revize edilmesi ve alınan ve/veya alınacak olan kararlarda kullanılan verilerin doğruluğunu artırır.

---

[23] Nurtaç ARSLAN, "İç Kontrol Sistemi Sunumu", T.C Strateji Geliştirme Başkanlığı http://www.strateji.gov.tr/ortak_icerik/strateji/ickontrolcalismalari/sunumlar/ickontrolicisleri sunumNurtacarslan.ppt, (16.04.2010), s.19.

[24] ARSLAN, a.g.e., s.6-7.

- ✓ İşletme bünyesinde oluşabilecek olan usulsüzlüklerin ve/veya usulsüzlüklerin önlenmesini ve tespit edilmesini sağlayarak, denetim çalışmalarına katkı sağlar.

- İşletmenin bulunduğu sektör kapsamında özel ve/veya genel mevzuata uyması gereken konularda katkı sağlar:

  - ✓ İşletme bünyesinde gerçekleştirilen periyodik ve süreç kontrolleri kapsamında yasal düzenlemelere uygunluğun sağlanmasına yardımcı olur.

İç kontrolün özel amaçları aşağıdaki belirtilen işlemlerden oluşmaktadır;[25]

Yetkilendirme: İşletmelere ait yürütülen faaliyetlerin işletme yönetiminin belirlemiş olduğu yetkilendirme kriterlerine paralel olarak uygulanmasını sağlamak, işletmeye ait varlıklara, kayıtlara, bilgi ve belgelere yönetim tarafından belirlenmiş olan yetkili kişiler tarafından ulaşabilirliğinin sağlanması,

Gerçeklik: İşletme bünyesinde gerçekleştirilen faaliyetlere ait faaliyet sonuçlarını yansıtan doğru işlem ve belgelerin sistem içerisinde kaydedilmesi ve belgelendirilmesi,

Bütünlük: İşletmedeki tüm işlemlerin belgelendirilmesini ve kaydedilmesini sağlamak,

Kayıtsal Doğruluk: İşlem sonuçlarına ait parasal değerlerin, doğru olarak kaydedilmesini sağlamak,

Sınıflandırma: İşlemlere ait oluşan parasal değerlerin finansal tablolar içerisinde yer alan hesap kalemlerinde doğru bir şekilde sınıflanmasının sağlanması,

---

[25] Vesile ÖMÜRBEK ve Sevil Özge ALTAY, "Turizm İşletmelerinde İç Kontrol Sisteminin Etkinliğinin İncelenmesi ve Manavgat Bölgesindeki Beş Yıldızlı Otellerde Bir Araştırma", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt:16, Sayı:1, 2011, s.382.

Zamanlılık: İşletmeye ait yürütülen faaliyet sonuçlarının faaliyetin gerçekleştiği dönem içerisinde yer almasının sağlanması, muhasebe kayıtlarının ilgili dönem içerisinde kayıt edilmesinin sağlanması,

Sorumluluk: İşletme içerisinde yer alan varlıklar ile varlıklara ait oluşturulan kayıt bilgilerinin periyodik olarak kontrol edilmesi ve karşılaştırılması gereklidir. Karşılaştırma işlemine ait ortaya çıkan farklılıkların tespit edilmesi, sorgulanması ve düzeltilmesi sağlanmalıdır.

İç kontrol kavramı, işletme içerisinde yapılması öngörülen kontrollere ait oluşturulan sistematik alt yapıyı ifade etmekle birlikte; yöneticinin işletmede yapılan ve tanımlanan işleri değerleme ve düzeltme faaliyeti olarak nitelendirilen kontrol kavramıyla örtüşmektedir.[26]

İşletme faaliyetlerinin, işletme misyon ve vizyonu ile uyum içinde düzenli ve verimli bir şekilde yürütülmesi, varlıkların korunması, hata ve hilelerin tespit edilip engellenmesi, muhasebe kayıtlarının tam ve doğru olması, güvenilir mali bilgilerin zamanında hazırlanması hedeflerine ulaşmak amacıyla oluşturulan tüm yöntem ve usullere **iç kontrol sistemi** denir.[27]

Uluslararası denetim standartlarına yön veren Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (The American Institute of Certified Public Accountants - AICPA) Denetim Standartları Kurulu (ASB)'nin yayınlamış olduğu 78 no.lu denetim standardında iç kontrol kavramı aşağıdaki belirtildiği gibi tanımlanmıştır.[28]

"İç kontrol, işletmenin yönetim kurulu, yönetici ve diğer personeli tarafından yönlendirilen ve aşağıda belirtilen amaçlara ulaşmak amacıyla yeterli ölçüde güvence sağlamak üzere oluşturulan bir süreçtir."

---

26 ÇATIKKAŞ, a.g.e., s.7.

27 Hakan BAKKAL ve Alper KASIMOĞLU, "İç Kontrol Sistemine Karşılaştırmalı bir bakış "COSO ve COCO Modeli", **Mevzuat Dergisi**, Sayı:178, Ekim 2012, s.1.

28 The American Institute of Certified Public Accountants Auditing Guide nr.78.

Uluslararası Sayıştaylar Birliği INTOSAI iç kontrolü şöyle tanımlamıştır;[29]

"İç kontrol; bir kurumun yönetimi ve personeli tarafından hayata geçirilen tamamlayıcı bir süreç olup, aşağıda sıralanan hedefleri gerçekleştirmek suretiyle; kurumun misyonunu başarması için riskleri göğüslemek ve makul bir güvence sağlamak üzere tasarlanmıştır:

- Faaliyetleri düzenli, ahlak kurallarına uygun, ekonomik, verimli ve etkin biçimde gerçekleştirme;

- Hesap verme sorumluluğunun gerektirdiği yükümlülükleri yerine getirme;

- Yürürlükteki yasalara ve yönetmeliklere uyma;

- Kayıplara, kötü kullanıma ve hasarlara karşı kaynakları koruma;

İç kontrol sistemini oluşturan temel unsurları aşağıdaki şekilde belirtmek mümkün olacaktır.[30]

- İyi bir örgüt yapısı

- Etkin bir muhasebe sistemi

- Yeterli sayı ve nitelikte personel

- İç denetim

Yukarıdaki belirtilen hususlar dikkate alındığında, işletme için etkili bir iç kontrol yapısının organizasyonunda bir başka önemli kriter ise işletme bünyesinde oluşturulan iç denetim ortamının bulunmasıdır.

---

29 INTOSAI, http://www.intosai.org/, (10.01.2014).

30 Gürdoğan YURTSEVER, "Bankacılığımızda İç Kontrol", **TBB Yayınları**, No:256, 2008, s.18.

İşletme bünyesinde oluşturulacak olan bir iç kontrol sisteminin özellikleri aşağıda maddeler halinde belirtilmiştir:[31] İç Kontrol,

- Yönetim sorumluluğu çerçevesinde sürekli ve sistematik bir şekilde yürütülmelidir.

- Bir yönetim aracı olmalıdır.

- Risk esasına dayalı olup, kontrol faaliyetleri gerekli yerde, zamanında ve gerektiği kadar yapılmalı ve uygulanmalıdır.

- Yönetimin bütün görevlilerini kapsamalıdır.

- Mali alanla sınırlı olmayıp, mali ve mali olmayan kontroller bütünü olmalıdır.

- Periyodik olarak (örn. yıllık olarak) değerlendirmeye tabi tutulmalıdır.

- Düzenleme ve uygulamalarında iyi mali yönetim ilkeleri esas almalıdır.

İşletme bünyesinde yer alan çalışanların organizasyonun faydasından çok kendi çıkarlarına yönelik faaliyetleri gerçekleştireceğinden hareket ile iç kontrol kavramı ortaya çıkmıştır. İşletme içerisinde yer alan iç kontrol yapısının etkinliğinin ve verimliliğinin oluşmadığı pozisyonlarda işletmelerin varlık kayıpları, işletme yönetiminin hatalı kararlar almasına buna bağlı olarak işletme bünyesinde kayıpların oluşmasına olanak sağlar. Bu bakımdan işletme içerisinde oluşturulan iç kontrol yapısı, işletmenin karşı karşıya kalacağı ve/veya kalabileceği risklerin minimize edilmesini sağlamakla birlikte; işletme bünyesinde görev alan işletme yöneticilerinin performanslarının ölçülmesi ve işlemlerin değerlendirilmesine yönelik fırsatlar yaratır.[32]

---

[31] M. Sait ARCAGÖK, "Yeni Mali Yönetim ve Kontrol Sisteminde İç Kontrol", **Maliye Bakanlığı Bütçe ve Mali Kontrol Genel Müdürlüğü**, Kızılcahamam, 09.09.2006, http://kontrol.bumko.gov.tr/Eklenti/4033,kizilcihamamsunumupdf.pdf?0, (07.08.2013), s.11.

[32] Ali ALAGÖZ, "İşletmelerde İç Kontrol Sisteminin Önemi ve Denetim Komiteleri ile İç Denetim Birimi İlişkisinin Hata ve Hilelerin Önlenmesindeki Rolü",

İç kontrol sisteminin tanımı içerisinde yer alan kavramlar değerlendirilmiş olup, iç kontrol sistemi aşağıda belirtilen kavramları ve bilgileri içermemektedir:[33]

1. İç kontrol dinamik yapısı gereği, statik bir yapıya sahip olan iç denetim faaliyeti ile aynı değildir.

2. İç kontrol yapısında gerçekleştirilen kontrol işlemleri ön bir mali kontrol olarak algılanmamalıdır.

3. İç kontrol, işletme bünyesinde oluşturulan yazılı prosedürler ile başlamamakla birlikte; iç kontrol, güçlü bir iç kontrol ortamının işletme bünyesinde oluşturulması ile başlar. Güçlü bir iç kontrol ortamının oluşturulmaması, yazılı hale getirilen prosedürlerin uygulanabilirliğini olumsuz yönde etkileyebilir.

4. İç kontrol, mali ön kontrol olmamakla birlikte, işletmelerin mali hizmetlerini yürüten birimler tarafından yapılması gereken bir iş değildir. İç kontrol sisteminin sahibi yönetimdir. İşletme bünyesinde faaliyetlere ait iç kontrol yapısının oluşturulmasından üst yönetim sorumludur. Yönetim; mali hizmetleri yürüten bölümlerden ve iç denetçilerden destek sağlar.

5. İç kontrol, işletmenin mali ve mali olmayan tüm fonksiyonlarını kapsamakla birlikte işletme bünyesinde görev alan bütün bölümleri ilgilendirir.

6. İç kontrol kapsamında bürokrasiye yer verilmez. İşletme bünyesinde oluşturulan kontroller çalışanların işlerini etkin ve verimli bir şekilde yapmasını sağlayan faaliyetlerden oluşur. Çalışanlar tarafından gerçekleştirilen faaliyetlere ait iç kontrol işlemleri faaliyetlere ilave olarak yapılan işler olarak sahiplenilmelidir. İşletme yönetimi tarafından işletme bünyesinde yürütülen faaliyetlerin bir parçası olarak kontroller tasarlanmalı ve uygulanması sağlanmalıdır.

---

http://www.alialagoz.com.tr/doc-dr-alialagoz-makaleleri/isletmelerde_ic_kontrol.pdf, (27.09.2011), s.4.

[33] İBİŞ ve ÇATIKKAŞ, a.g.m., ss.98.

7. İşletme bünyesinde yürütülen karmaşık, basit ve/veya önemli görülmeyen bütün faaliyetlerde iç kontrol sistemine ihtiyaç duyulur. Ancak bu noktada dikkat edilmesi gereken, tasarlanan ve uygulanacak olan kontrollerin niteliğinin fayda sağlayacak konumda olması sağlanmalı, bu kriter kapsamında gerekli kontroller tasarlanmalıdır.

8. İç kontrol yapısının uygun ve verimli bir şekilde sağlam olarak tasarlanması işletme kaynaklarının etkin kullanıldığı, yolsuzluk olmayacağı ve mali tabloların doğruluğunun tam olduğunu göstermemektedir. İşletme bünyesinde yer alan iç kontrol yapısı kesin güvence vermemekle birlikte; işletme hedeflerine ne derece ulaşılacağı ile ilgili olarak makul güvence verir.

1.4.2 İç Kontrol Kavramının Önemini Artıran Gelişmeler

Bankacılık sektörünün dünya piyasasında maruz kaldığı ve analiz etmek durumunda olduğu risk sayısı ve çeşitleri artış göstermiştir. Bankacılık sektöründe gün geçtikçe ortaya çıkan yeni ürün çeşitliliği, bankaların kullandığı bilgi sistemlerine ait yenilikler, ulaşılan ve oluşan yeni finansal pazarlar, uluslararası düzeyde bankalara bilinmeyen ortaya çıkmayan imkânlar sunmakla birlikte, banka bünyesinde yeni risklerin ortaya çıkmasına neden olmuştur.

Risk yönetimi ve iç kontrol kavramlarının finans piyasalarının tamamında ve bankacılık sektöründe önemli hale gelmesinin en önemli nedeni, 1980-1990 arası dönemde, uluslararası ve yerel olarak birçok finans piyasasında rol alan bankalarda oluşan ve önemli kayıpların oluşmasına neden olan olaylar ve krizlerdir. Belirtilen periyot içerisinde birçok işletme, iç yapılarında uyguladıkları kontrol ve risk yönetim sistemlerinde yaşadıkları başarısızlıklar sebebiyle birden fazla risk ve problemlerle karşı karşıya kalmışlardır. Sektörel olarak yaşanan olaylar, kontrol faaliyetleri konusunda dünya genelinde bir farkındalığın yaşanmasını sağlamıştır. Özellikle bankalardaki problemlerin en temel nedenin banka faaliyetlerinden sorumlu olan üst yönetiminin ve/veya paydaşları tarafından bankanın ulaşamayacağı hedeflerin ve stratejilerin belirlenerek, ölçüm kriteri olmayan şekilde yüksek düzeyde risk alınmasıdır. Yüksek düzeyde belirlenen risklerin yanında söz konusu bu riskleri minimize edecek ve

izlenebilirliğini sağlayacak olan iç kontrol sistemleri tasarlanmamış veya tasarlanan sistemlerde büyük hata ve açıkların oluştuğu tespit edilmiştir. Belirtilen bu kriterlere en uygun örnek olarak, Barings Bank'ın iflas etmesi ile sonuçlanan durum verilebilir. Barings Bank olayı söz konusu bankanın Singapur bölgesindeki bölümde gerçekleşmiştir. Söz konusu bölümde görevli ve güvenilir çalışan olan Nick Leeson Nikkei endeksinde yetkilendirilmemiş future ve opsiyon pozisyonları alması sonucunda söz konusu bankanın iflasına kadar olan sürecin oluşmasına neden olmuştur. İlgili personel tarafından yetkilendirilmemiş olan future ve opsiyon pozisyonlarının alınması sonucunda, 1 Milyar USD'yi aşan bir kayıp ortaya çıkmış olup, bunun sonucu olarak ilgili banka 26 Şubat 1995 tarihi itibariyle iflas etmiştir.[34]

Barings Bank'ta yaşanan ve dünya gündemini meşgul eden ve yüksek miktarda zarara yol açan işlemler incelenip, değerlendirildiğinde ortaya çıkan zararların banka bünyesindeki büyük kontrol eksikliğinden ve etkili olmayan bir yönetim yapısından kaynaklandığı ortaya çıkar. Bu değerlendirmenin en önemli yapı taşı Leeson'un işlemleri yürüten yapıyı ve işlemleri yürüten yapı dışında arka ofis işlemlerini de kontrol etmesidir. Nick Leeson bu kontrolü elinde tutarak; rahatça pozisyon alabiliyor, pozisyonu istediği şekilde yönetebiliyor ve yapmış olduğu işlemlere ait oluşan zararları banka bünyesindeki fiktif nitelikteki hesaplarda gizleyebiliyordu.

Barings Bank konusu değerlendirildiğinde, gerçekleştirilen operasyonlara bağlı olarak aşırı karlılık, belirlenen limit miktarlarının dikkate alınmaması ve buna bağlı olarak fon talebi büyüklüğünün ve sıklığının artış göstermesi ortaya çıkan en temel risk göstergelerini oluşturmaktadır. Yaşanan olay içerisinde yapılan işlemler ve faaliyetler analiz edildiğinde, aşağıdaki belirtilen hata ve aksaklıkların gerçekleştiği görülmektedir:[35]

- Üst yönetim tarafından banka bünyesindeki stratejinin sağlıklı olarak belirlenmemesine bağlı olarak tam, doğru, zamanında ve yeterli bir seviyede risk analizi yapılmayan bir faaliyet alanında işlem yapılması,

---

34 YURTSEVER, a.g.e., s.19-20.

35 OpRisk Dergisi, "Barings Bank'ın İflas Öyküsü", http://www.opriskdergisi.com/oprisk-ornek-22-barings_bankin_iflas_oykusu.html, (24.03.2014), s.2.

(yeni ürün/faaliyet sürecinin bulunmaması, içeriği ve riskleri anlaşılmayan ürünlerle sektör içerisinde operasyonel işlemlere başlanması)

- Gerçekleştirilen operasyonlarda görevler ayrılığı ilkesinin dikkate alınmayarak, işlemlerin yürütülmeye çalışılması (örneğin, alım-satım işlemlerinin ve operasyon masasına ait işlemlerin banka bünyesinde tek bir kişinin sorumluluğuna bırakılması)
- İşletmenin ve işletmeye bağlı grup düzeyinde kontrol mekanizmalarının tam, doğru, zamanında ve sağlıklı bir şekilde çalışmaması,
- İşletme bünyesinde kabul edilen limit tahsis seviyelerinin oluşturulmaması, yasal mevzuat gereği oluşturulması ve kontrol edilmesi gereken limit değerlerinin takip edilmemesi,
- İşletme bünyesinde gerçekleştirilen raporlama işlemlerinin gerçekleştirilmesine rağmen, raporlama yapılan Yönetim Kurulu'nun üyelerinin yetkin olmaması buna bağlı olarak görevini yeterli bir şekilde yapmaması,
- Banka bünyesinde yer alan iç denetim bölümünün üst yönetimin kendisinden beklediği görevleri yerine getirememesi buna bağlı olarak, etkin ve verimli bir şekilde çalışmaması,
- Banka bünyesinde ve menkul kıymet işletmesine personel kaynağı sağlanmasında insan kaynakları bölümünün ve yönetiminin yetersizliğidir.

İşletmelerin faaliyetlerini yürütmesinde önemli bir rol oynayan iç kontrol kavramının önemini artıran bir diğer olay ise Parmalat olayıdır. Parmalat firması, Parmalat Grup'a ait temel gıda ve süt ürünlerinin üretilmesini ve satış işlemlerinin yürütülmesini sağlayan bir firmadır. 2002-2005 yılları arasında bünyesinde toplam 67 adet işletmenin yönetiminden direkt sorumlu olmuştur. Parmalat işletmesinde ortaya çıkan kontrol zayıflıkları aşağıdaki belirtilen durumların ortaya çıkmasına neden olmuştur:[36]

[36] Ceren Ayça GÖÇEN, "Kurumsal Yönetim, İç Kontrol ve Bağımsız Denetim: Parmalat Vakası", **Mali Çözüm Dergisi**, Sayı: 97, 2010, s.117.

- **Sahte ve gerçekliliği olmayan belgelerin düzenlenmesi:** İşletme bünyesinde gerçek olmayan muhasebe işlemleri gerçekleştirilmiş, işletme bünyesinde geçerli olmayan müşteri cari kartları oluşturulmuş ve sahte evraklar oluşturulmuştur. Açılan sahte hesaplar Parmalat işlemesinde görev alan birçok üst yöneticinin cari hesapları dilediği şekilde kullanmasına olanak sağlamış, buna bağlı olarak gerçekte olmayan işlemlerin oluşturulmasına imkân tanımıştır. Açılan hesapların finansal faaliyetlere ait kontrollerde ortaya çıkmaması amacıyla bazı yöneticiler tarafından çalışanlara ödeme yapılarak yöneticiler tarafından işletme kayıtlarının tam ve doğru bir şekilde sunulmasını engellemiştir.[37]

- **İşletmeye ait borç miktarının manüple edilmesi:** Parmalat olayında, işletme yüksek tutardaki borç miktarını (9.1 milyar euro) gerçekte olan borç miktarından daha az göstermiştir. Bu işlemleri gerçekleştirirken, belli bir tutardaki borcu iştiraklerine borç olarak, belli bir miktardaki tutarı da sabit kıymetler için ayrılan sermaye olarak göstermiştir. Yapılan bu işlem sonucunda gerçekte var olmayan işlemlere bağlı olarak finansal tablolarda yer alan borç miktarında azalma sağlamıştır. Bu işlemleri; şirket kayıtlarında borç kaydı yapmadan ve borcun sermaye olarak kayıt edilmesi şeklinde gerçekleştirmiştir.[38]

- **İşletme bünyesinde türev ürünlerin kullanılması:** İşleme tarafından işletme bilançosunu desteklemek amacıyla türev araçları ve ürünleri kullanılmıştır. Citigroup ve Merrill Lynch gibi ticari bankaların yayınlamış olduğu finansal enstrümanlar, Parmalat Grup'un mali tablosunda finansal yapısının hatalı olarak gösterilmesine olanak sağlamakla birlikte; firmaya finansal kaynak sağlamıştır.[39]

- **Satış faaliyetlerinde yapılan operasyonlar:** Satış operasyonları sonucunda oluşan zarar miktarı, işletmeye bağlı olan diğer şirketler kullanılarak, işletmenin aktif değeri olduğundan daha iyi gösterilmiştir. Söz konusu bu işlem kapsamında işletmeye bağlı olan iştirakler yardımıyla, tahsilat imkânı bulunmayan ve/veya vadeye bağlı olarak tahsilat değeri azalan alacak miktarları saklanmıştır. İşletme

---

37 GÖÇEN, a.g.m., ss.117.

38 GÖÇEN, a.g.m., ss.118.

39 GÖÇEN, a.g.m., ss.119.

tarafından kaynak olarak kullanılan krediler, işletmeye bağlı olan iştirakler kullanmış gibi gösterilerek kredi giderlerinin gizlenmesi sağlanmıştır. İşletme bünyesinde gerçekte olmayan gelir kayıtları, gerçekte olmayan müşterilerin sistem içerisinde yer alması sağlanarak oluşturulmuştur. Satış faaliyetleri değerlendirildiğinde, çift faturalama işlemlerinin oluşturulduğu işletmeye ait iştiraklere gerçekte olmayan satış işlemlerinin yapıldığı ve satış fatura bedellerinin olması gereken tutardan daha fazla tutarda kesildiği görülmüştür.[40]

İç kontrol işlemlerinin önemli ve kritik bir süreç olduğunu gösteren diğer bir olay Enron olayıdır. Enron şirketi tarafından gerçekleştirilen finansal raporlama işlemine ait tutarsızlık ve aksaklıklar söz konusu işletme ile ilgili literatüre geçecek olan olayın yaşanmasına neden olmuştur. Enron şirketi ortaklarına ve bağlı olduğu regülasyona ait yapmış olduğu gelir raporlamalarında farklı bilgiler aktarmıştır. Ortaklarına fazla gelir ettiğini raporlamasına rağmen, ilgili yasal kuruluşlara (vergi dairelerine) zarar ettiğini raporlamıştır.

Şirketin sahip olduğu toplam aktiflerinin üçte bir oranı çalışanlara ait emeklilik fonlarından oluştuğu, oluşan iflas durumu ile birlikte çalışanlar işsiz kalmanın yanı sıra işletme bünyesinde yapmış oldukları birikimleri de kaybetmişlerdir. Şirket; bünyesindeki finansal tablolarda oluşan kayıp miktarlarını azaltarak, işletme karının arttırılması hedeflenmiştir. Karın arttırılması amacıyla; işletmeye ait hisse senetleri bir başka şirkete transfer edilerek, faaliyet gösterdiği enerji sektöründeki kredi seviyesi azaltılmış ve borç miktarının bilanço içerisinde yer almaması sağlamıştır.[41]

WorldCom şirketinde yaşanan durum, aynı Enron olayında olduğu gibi 1996–2000 dönemi içerisinde ortaklarına ve bağlı bulunduğu vergi dairelerine farklı şekilde kar raporlaması şeklinde gerçekleşmiştir.

---

40 GÖÇEN, a.g.m., ss.119.

41 Mustafa ARI, "Finansal Raporlama Skandalları ve Mali Tabloların Güvenirliliği", http://birimler.dpu.edu.tr/app/views/panel/ckfinder/userfiles/17/files/DERG_/23/409-420.pdf, (07.07.2015), s.1.

Sorumlu olunan alanlarda farklı şekilde ve miktarda raporlama yapılması nedeniyle işletmeye ait mali tablo kullanıcılarının güvenlerinin sarsıldığı görülmüştür. İşletme ile ilgili olarak oluşan olaylara ait ayrıntılı bir değerlendirme yapıldığında, mali tablolara olan güvenin olumsuz yönde etkilenmesinin nedeni, işletme bünyesinde oluşan kurumsal yönetim başarısızlıklarından kaynaklandığı tespit edilmiştir.

Amerika kamuoyunda oluşan muhasebe ve mali denetim skandalları Amerikan piyasasında yer alan yatırımcıların güvenini olumsuz yönde etkilemiştir. Amerika'daki faaliyet gösteren işletmelerin düzenlemiş olduğu mali tabloların güvenirliliğini arttırmak ve söz konusu mali tabloların denetim faaliyetlerini iyileştirmek amacıyla; 30 Temmuz 2002 tarihinde "Sarbanes-Oxley Yasası" oluşturulmuştur.[42] Amerika içerisinde halka açık olan işletmelerle, söz konusu işletmelerin denetim faaliyetini gerçekleştiren denetim firmalarını ilgilendiren yasa, denetim firmalarında görev alan denetçilerin ve denetlenen şirketlerde çalışan muhasebeci ve iç denetçileri kapsamaktadır.[43]

Finansal piyasalarda ortaya çıkan bu olaylar, iç kontrol kavramının önemini artırmakla birlikte işletmeler içerisinde denetçinin uygulaması gereken kriterlerin ortaya çıkmasını sağlamıştır. Bu olaylar, iç kontrol yapısı ile birlikte finansal tablo kullanıcılarına güvenilir finansal rapor hazırlanmasını sağlamıştır. Onaylanan kanun kapsamında temel ilke olarak, işletmenin belirlemiş olduğu hedefleri yerine getirebilmesi için işletme kaynaklarının etkin ve verimli olarak kullanılması belirlenmiştir. Bu kapsamda, işletme faaliyetlerine ait operasyonel kontrollerin yapılması, operasyon sonuçlarına ait finansal tabloların kanun ve düzenlemelere uygun olması sağlanmaktadır. Bu durumun oluşabilmesi için, uygunluk denetimlerinin yapılmasını temel kriter olarak belirlenmiştir.

---

42 Handan ERZİ, "Sarbanes-Oxley Yasasının Yolsuzluk Vakalarının Ortaya Çıkarılmasındaki Rolü: Yasa Öncesi ve Sonrasında Yaşanan Şirket Yolsuzluk Vakaları Üzerine Mukayeseli Bir İnceleme", **Yüksek Lisans Tezi**, Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü, Hatay, 2010, s.29.

43 Ayça Zeynep SÜER, "Profesyonel Muhasebe Mesleğinde Enron Skandalı ve Sonrası Gelişmeler", **VI. Türkiye Muhasebe Denetimi Sempozyumu**, Antalya, 16-20 Nisan 2003, s.118.

İç kontrol sistemi içerisinde aksaklıklara istinaden Enron ve WorldCom'a ait finansal tablolarda yaşanan sıkıntılar nedeniyle Sarbanes-Oxley Yasası ("SOX") 404. bölümüne göre, finansal raporlamada iç kontrolün etkinliğinin değerlendirilmesi ve değerlendirme sonuçlarının raporlanmasının önemli olduğu ve halka açık işletmelerde bu durumun zorunlu hale getirilmesi sağlanmıştır.

1.4.3 İç Kontrol Sistemi İle İlgili Düzenlemeler

İç kontrol sisteminin önemini artıran gelişmeler ile birlikte ulusal ve uluslararası anlamda birçok düzenlemeye gidilmiştir. Bu düzenlemeler aşağıdaki gibidir:

COSO Düzenlemeleri: Kontrol ve iç kontrol kavramı açıklanmaya çalışıldığında ilk olarak COSO uygulaması dikkate alınır. COSO uygulamasının gerçekleştirdiği en önemli iç kontrol çalışması 1987-1997 dönemi arasında yapılmış olup, çalışma içerisinde Amerika'da faaliyet gösteren halka açık şirketlerin yanıltıcı ve hatalı finansal raporları analiz edilmiştir.[44] İlgili dönemlerde yapılan çalışmaya ek olarak ilgili kurum tarafından "İç Kontrol ve Bütünleşik Sistem" adlı rapor yayınlanmıştır. Rapor içerisinde ideal uygulanması gereken iç kontrol sistemi modeline yer verilmiştir. 1992 yılında yayınlanan bu model, dünya genelinde faaliyet gösteren işletmeler tarafından kabul edilmiştir. İç kontrol sistemine ilişkin yayınlanan diğer çalışmalar; "Guidance on Monitoring Internal Control Systems"[45] ve küçük işletmeler için oluşturulan "Internal Control Over Financial Reporting — Guidance for Smaller Public Companies" adlı çalışmalardır.[46] COSO Raporu'nda iç kontrol; kurumun yönetim kurulu, yönetimi ve diğer personeli tarafından gerçekleştirilen, faaliyetlerin etkinliğini ve verimliliğini sağlama, güvenilir finansal raporlama ve ilgili kanunlara ve düzenlemelere uygun olma hedeflerine ulaşmak amacıyla oluşturulan bir süreç olarak tanımlanmaktadır.[47]

---

44 COSO, "Fraudulent Financial Reporting: 1987-1997 An Analysis of U.S Public Companies", http://www.coso.org/documents/FFR_1987_1997.PDF, March 1999, (09.07.2014), s.4.

45 COSO, "Internal Control-Integrated Framework-Guidance on Monitoring Internal Control Systems", http://www.coso.org/documents/volumeii-guidance.pdf , June 2008, (09.07.2014), s.1-54.

46 COSO, "Internal Control Over Financial Reporting Guidance for Smaller Public Companies", http://www.coso.org/documents/sb_executive_summary.pdf , June 2006, (09.07.2014), s.12.

47 Münevver YILANCI, **İç Denetim: Türkiye'nin 500 Büyük Sanayi İşletmesi Üzerine Bir**

Uluslararası İç Denetçiler Enstitüsü (IIA) Düzenlemeleri: İşletme bünyesinde oluşturulan iç kontrol yapısının varlığını sürdürmesi ve etkin ve verimli bir şekilde işletme bünyesinde çalışması için iç denetçiler önemli rol oynamaktadır. Bu kapsam dahilinde; IIA tarafından 01.01.2004 tarihinde oluşturulan uluslararası iç denetim standartları ile iç denetçilerin rol ve sorumlulukları tanımlanmıştır. Bu standart hazırlanırken, standart içerisinde belirtilen kriterlerin uygulanabilmesi için temel uygulama alanlarının belirlenmesi, iç denetim faaliyetlerinin gerçekleştirilmesine bağlı olarak standart bir çerçeve oluşturarak, iç denetim faaliyetini uygulayan sorumluların performanslarının belirlenen kriterler kapsamında değerlendirilmesi amaçlanmıştır. İlgili standartlarda iç kontrol sisteminin kurulması, izlenmesi ve değerlendirilmesine ilişkin düzenlemeler yapılmıştır. Uygulanması planlanan standartlar; nitelik standartları, performans standartları ve uygulama standartları olmak üzere üç bölüm içerisinde sınıflandırılmıştır.[48]

Amerikan Sermaye Piyasası Kurulu (SEC) Düzenlemeleri: SEC tarafından yayınlanan Sarbanes Oxley yasasında iç kontrol kavramına ilişkin düzenlemeler yapılmıştır. Yapılan düzenlemenin kapsamı diğer yapılan düzenlemelere göre daha sınırlıdır. SEC tarafından yapılan düzenleme içerisinde yatırımcıların daha doğru bilgilendirilmesine yönelik yapının işletme bünyesinde oluşturulması vurgulanmıştır. Yatırımcıların bilgilendirilmesinin dışında yatırımcı hak ve menfaatlerinin zedelenmemesi amacıyla; denetim komitesinin faaliyetlerinin etkinliğini ve verimliliğini arttırmanın yanı sıra; denetçilerin bağımsız olmalarının sağlanmasına ait görev ve sorumlulukların işletme yönetiminde olduğu belirtilmiştir. Düzenleme kapsamında, üst yönetim tarafından finansal raporlama sürecine ait iç kontrol sisteminin etkinliği ve verimliliği ile ilgili olarak güvence vermesi talep edilmiştir. İşletme içerisinde iç kontrol sisteminin oluşturulması ve verimliliği sağlama görevinin işletme yönetiminde olduğu belirtilmiştir. Belirtilen sorumluluklar kapsamında; üst yönetim tarafından işletme

---

Araştırma, Nobel Yayın Dağıtım, 2. Baskı, Eskişehir, 2006, s.28.

[48] Duygu Anıl KESKİN, **İç Kontrol Sistemi Kontrol Öz Değerlendirme**, Beta Yayınları, İstanbul, 2006, s.32.

içerisinde yer alan iç kontrol sistemine ait kontrol aksaklıklarının ve zayıflıklarının denetim faaliyetini yürüten denetim personeline iletmek zorunda olduğu belirtilmiştir.[49]

Uluslararası Yüksek Denetleme Kuruluşları Örgütü (INTOSAI) Düzenlemeleri: İç kontrol standartları komitesi tarafından iç kontrol kavramına ait uygulama rehberi yayınlanmıştır. Söz konusu rehberin oluşturulmasındaki asıl hedef; işletmeler bünyesinde yer alan iç kontrol faaliyetlerin etkili bir şekilde oluşturulması ve sürdürülmesi ile ilgili olarak genel bir çerçeve oluşturmaktır. Rehber içerisinde kamu denetçilerinin iç kontrol faaliyeti ile ilgili olan rolleri ve sorumlulukları açıklanmıştır. Uygulama içerisinde iç kontrol uygulamalarının tanımlanması gerektiği iç kontrol sisteminin etkinliğinin sağlanması gerektiği belirtilmiştir.[50]

Treadway Komisyonu Düzenlemeleri: İlgili düzenleme kapsamında işletmenin operasyonel sonuçlarının yer aldığı finansal raporlama süreci içerisinde karşılaşılabilecek olan hata ve hilelerin oluşmaması adına; etkin bir iç kontrol sisteminin kurulması gerektiği belirtilmiştir.[51]

Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (AICPA) Düzenlemeleri: AICPA tarafından işletme için verimli olacak bir denetim çalışması yapılabilmesi için gerekli olan kriterleri tanımlayan genel kabul görmüş denetim standartları (GKGDS), genel standartlar, çalışma alanı standartları ve raporlama standartları olmak üzere toplam on adet standart oluşturulmuştur. Oluşturulan standartlar içerisinde yer alan çalışma alanı standartları kapsamında iç kontrol sistemi ile ilgili olarak açıklamalara yer verilmiş olup, denetim çalışmasının planlanması, kapsam çerçevesinin oluşturulması ve bir sonraki gerçekleştirilecek olan denetim çalışmalarına destek olması amacıyla dış denetçiler tarafından işletmenin iç kontrol sistemini değerlendirmeleri önerilmiştir.

---

49 Sarbanes-Oxley Act, "Public Law 107-204", https://www.sec.gov/about/laws/soa2002.pdf, July 30, 2002, (09.06.2015), s.1-66.

50 KESKİN, a.g.e., s.38.

51 COSO, "Report of the National Commission on Fraudulent Financial Reporting", http://www.coso.org/Publications/NCFFR.pdf, October 1987, (12.06.2014), s.34-40.

Uluslararası Muhasebeciler Federasyonu (IFAC) Düzenlemeleri: IFAC tarafından GKGDS'nın daha detaylı açıklamaları olan uluslararası denetim standartları (ISA) yayınlamıştır. Uluslararası denetim standart numarası 400 olan bölüm, standart risklerin belirlenmesi ve iç kontrol kavramı ile ilişkili olarak oluşturulmuştur. Standart kapsamında COSO düzenlemesi içerisinde yer verilen iç kontrol tanımına benzer bir tanım yapılmıştır. Standart içerisinde, denetçinin denetim faaliyetini tam, doğru, zamanında ve standartlara uygun bir şekilde yapabilmesi için işletmeye ait iç kontrol yapısını tanıması gerektiğine yer verilmiştir. Standart içerisinde iç kontrol sisteminin bazı sınırlamalara sahip olduğuna yer verilmiştir. Bu sınırlamalardan bazıları şunlardır:[52]

- Beklenen faydaların iç kontrol maliyetinden fazla olacağına dair yönetimin beklentisi,
- Dikkatsizlik, dalgınlık, yanlış karar verme ve talimatların yanlış anlaşılmasından kaynaklanan insan hatalarının gerçekleşme olasılığı,
- Yönetimden bir üyenin veya işletme çalışanlarının birinin şirketin içinden veya dışından bir grupla yapılacak gizli anlaşmayla, iç kontrolleri yanıltması olasılığı,
- İç kontrolün uygulanmasından sorumlu kişinin sorumluluğunu kötüye kullanma olasılığı,
- Şartların değişmesinden dolayı mevcut prosedürlerin yetersiz kalması ve prosedürlere uygunluğun bozulmasıdır.

Basel II Düzenlemeleri: Finansal raporlama sürecinde şeffaflık amaçlanarak, BIS (Bank for International Settlements) tarafından 2004 yılında oluşturulan Basel II ilkeleri oluşturulmuştur.[53] İç kontrol sistemlerinin etkinliğinin sağlanması ile ilgili olarak belirli kriterler belirlenmiştir. Bu kriterler;[54]

---

52 Tamer AKSOY, "Ulusal ve Uluslararası Düzenlemeler Bağlamında İç Kontrol ve İç Kontrol Gerekliliği: Analitik Bir İnceleme", **Mali Çözüm Dergisi**, Sayı: 72, 2005, s.241-243.

53 Süleyman UYAR ve Hakan AYGÖREN, "Basel II İlkelerinin KOBİ'lere Olası Etkileri: Finansman Maliyeti, Finansal Raporlama ve Muhasebe Açısından Değerlendirme", **Mali Çözüm Dergisi**, Sayı: 77, Ağustos-Eylül-Ekim 2006, s.53.

54 Güler ARAS, "Basel II Bankacılık Düzenlemeleri ve İç Denetim", **TİDE İç Denetim Dergisi**, Sayı:17, 2007, s.24-25.

a) Banka yönetimi, banka içerisinde yer alan iç kontrol yapısına ait sistemin kurulmasından sorumlu olmakla birlikte, oluşturulan iç kontrol sisteminin yeterliliğini değerlendirir.

b) Banka içerisinde yer alan iç kontrol sistemi, işletme bünyesinde yürütülen işlemlerin işletme stratejileri ile verimli bir şekilde yürütülmesini sağlamakla birlikte bu işlemlere ait iç denetim faaliyetlerinin yerine getirilmesi için yardımcı olur.

c) İç kontrol sistemi bankanın devamlılığı dikkate alınarak süreklilik gösteren bir fonksiyona sahip olmakla birlikte, bu fonksiyonu yerine getirebilmesi için bağımsız bir yapıya sahip olmalıdır.

d) Banka bünyesinde oluşturulan iç kontrol yapısının banka bünyesinde uygulanabilmesi ve banka bünyesinde uygulanabilirliğinin yaygın hale getirilebilmesi ve devamlılığının sağlanabilmesi amacıyla iç kontrol yönetmeliği oluşturulmalıdır.

e) İç kontrol sistemi profesyonel yeterliliğe sahip olmalıdır.

f) İç kontrol sistemi işletmenin karşılaştığı riskleri değil, ilerleyen zamanlarda karşılaşabileceği riskleri analiz etmeli, ölçmeli ve değerlendirmelidir.

g) Banka yapısına göre oluşturulan iç kontrol sisteminin oluşturulmasından yönetim kurulu, üst yönetim sorumlu olmakla birlikte; oluşturulan iç kontrol sisteminin uygun çalışmasından iç denetim bölümü başkanı sorumludur. Yönetim kurulu ve üst yönetimin iç kontrol sisteminin periyodik olarak gözden geçirmesini sağlamalıdır.

h) Yönetim kurulu, üst yönetim ve iç denetim bölüm başkanın yanında denetim komitesinin oluşturulması iç kontrol sistemini güçlendirir.

ı) İç kontrol sisteminin oluşturulması ve işletme bünyesinde faaliyete geçirilmesi ile ilgili olarak konusunda uzman olan dış kaynaklardan hizmet alınabilir.

Türk Ticaret Kanunu Düzenlemeleri: Uygulamaya alınan Türk Ticaret Kanunu ile birlikte denetim faaliyetinin işlevi ve kapsamında değişiklikler yapılmıştır. Kanun kapsamında, uluslararası finansal raporlama standartlarına (UFRS) uygun finansal

raporların üretilmesi amacıyla, işletme yönetimine ve denetçilerine bir takım sorumluluklar getirilmiştir. Yapılan düzenleme ile birlikte işletmelerin TTK ve UFRS'ye uygun Türkiye Finansal Raporlama Standartları (TFRS) ile uyumlu finansal tablolar hazırlamaları uygun görülmüştür. Düzenlenen kanun kapsamında yer alan maddeler değerlendirildiğinde; iç kontrol sistemi ve iç kontrol sisteminin etkinliği ile ilgili bir inceleme yapılması gerektiği konusunda açık bir ifadeye yer verilmemiştir. Kanun kapsamında, işletmenin yatırımcılara doğru bilgi verebilmeleri açısından etkili bir iç kontrol yapısına sahip olmaları gerektiği sonucuna varılmaktadır.[55]

Sermaye Piyasası Kurulu Düzenlemeleri: Seri: X, No: 16, Sermaye Piyasasında Bağımsız Denetim Hakkında Tebliğ, Seri: X, No: 19, Sermaye Piyasasında Bağımsız Denetim Hakkında Tebliğde Değişiklik Yapılmasına Dair Tebliğ, Seri: X, No: 22, Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ ve Seri: X, No: 23, Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğde Değişiklik Yapılmasına Dair Tebliğ ve 22 numaralı tebliğin 10. Kısmı içerisinde iç kontrole ilişkin başlıca düzenlemelere yer verilmiştir. SPK tarafından işletmelerin yatırımcılara verdiği bilginin tamlığı, doğruluğu ve güvenirliği ile ilgilendiğinden; iç kontrol yapısı ve sistemi genel olarak dış denetim açısından ele alınmıştır. SPK tarafından düzenlenen tebliğler genel anlamda SEC tarafından yapılan uygulama ve düzenlemelerle uyumlu olarak ortaya çıkmaktadır. SPK tarafından oluşturulan tebliğlere göre, iç kontrol yapısı işletmeye ait dış denetim faaliyetini sağlayan dış denetim çalışanlarına işletme içerisinde gerçekleştirilecek olan denetim kapsamının, zamanlamasının ve işletmeye ait risklerin tespit edilmesine katkıda bulunur. Bu faydanın sağlanabilmesi açısından, iç kontrol sisteminin yapısı, üst yönetimin belirlemiş olduğu faaliyet hedeflerinin hayata geçirilmesi bakımından, faaliyetler için olumsuz durumlar oluşturabilecek olan risklerin, önceden tespit edilmesi için dizayn edilmelidir. SPK tebliğlerinde yer alan tanımlamaya göre; işletmenin kontrol çevresi içerisinde gerçekleştirilen, süreçlere ait risk analiz etme, finansal raporlama ve iletişim süreçlerine bünyesinde yer veren sistem iç kontrol sistemi olarak tanımlanmıştır. İç kontrol sistemi içerisinde bilgi sistemlerinin, tasarlanan kontrol faaliyetlerinin izlenmesi işlemleri yer alır. Denetim faaliyetini gerçekleştiren sorumlu kişi

[55] KESKİN, a.g.e., s.50.

tarafından işletme içerisinde tasarlanmış ancak işletme faaliyetleri için verimli ve etkili olmayan bir iç kontrol yapısı tespit edilmesi durumunda, tespit edilen bu durumun iç kontrol yapısından sorumlu olan işletme üst yönetimine iletilmesi sağlanır.

1.4.4 Bankacılık Sektöründe İç Kontrol Kavramı

Banka iç kontrol sistemi, banka yönetim kurulu, banka yöneticileri ve diğer banka personelinden etkilenen bir süreçtir. Banka iç kontrol sistemi, banka bünyesinde uygulanan prosedür ve politikalar kapsamında nitelendirmenin yerine; banka bünyesinde operasyonların devamlılığı ve sürekliliği için önem taşıyan ve banka bünyesinde görev alan tüm çalışanların iştirak etmesiyle uygulanan bir yapıdır. Bu yapının sistematik bir alan içerisinde oluşturulması, geliştirilmesi ve kurumsal yapının buna ayak uydurması sağlanmalıdır.[56]

Türkiye bankacılık sektöründeki iç kontrol kavramının uygulama aşamaları incelendiğinde; 01 Kasım 2005 tarihinde uygulanmaya başlanan 5411 sayılı Bankacılık Kanunu'nu içerisindeki ikinci bölüm içerisindeki "İç Sistemler" konu başlığı altında bankalar tarafından oluşturulması gereken iç sistemler (iç kontrol, iç denetim ve risk yönetimi sistemleri) hakkında yerine getirmesi gereken yükümlülükler belirtilmiştir. Kanunun 29. maddesi içerisinde "Bankalar, maruz kaldıkları risklerin izlenmesi, kontrolünün sağlanması, faaliyetlerinin kapsamı ve yapısıyla uyumlu ve değişen koşullara uygun, tüm şube ve konsolidasyona tabi ortaklıklarını kapsayan yeterli ve etkin bir iç kontrol, risk yönetimi ve iç denetim sistemi kurmak ve işletmekle yükümlüdürler. İç kontrol, risk yönetimi ve iç denetim sistemlerinin kuruluşuna, işleyişine, yeterliliğine, oluşturulacak birimlere, icra edilecek faaliyetlere, üst yönetimin görev ve sorumlulukları ile Bankacılık Düzenleme ve Denetim Kurumuna yapılacak raporlamalara ilişkin usul ve esaslar kurulca belirlenir" ifadesine yer verilmiştir. 5411 sayılı kanun içerisinde iç kontrol, iç denetim ve risk yönetim sistemleri, toplu bir şekilde iç sistemler olarak tanımlanmıştır. 5411 sayılı kanun kapsamında iç sistemler bir önceki uygulanan kanun içeriklerine göre daha kapsamlı ve detaylı olarak açıklanmıştır. Kanunun 30. madde

[56] Basel Committee on Banking Supervision, " The Internal Audit Function in Banks", June 2012, s.21.

içerisinde "iç kontrol faaliyetlerinin yönetim kuruluna bağlı olarak çalışacak iç kontrol birimi ve personeli tarafından yürütülmesi" ifadesi ilk kez bir kanun maddesi olarak düzenlenmiştir.[57]

1.4.5 Denetim Standartları Kapsamında İç Kontrol Sistemi

İç kontrol sistemi, denetim faaliyetlerini gerçekleştiren bağımsız denetçiler açısından önemli bir kavram olarak ortaya çıkmaktadır. Denetim faaliyetini yürüten denetçi açısından denetim riskini değerlendirirken dikkate alacağı hususlar bulunmaktadır. Denetçinin denetim riski kapsamında aşağıdaki belirtilen denetim standartlarında yer alan konuları dikkate almalıdır.

Denetçinin muhasebe ve iç kontrol sistemi ile ilgili olarak yeterli bilgi seviyesine sahip olması denetim çalışmasının planı ve etkililiği için önemlidir. Muhasebe ve iç kontrol sistemi ile ilgili yeterli bilgiye sahip olunması, denetim faaliyetine ait denetim risk değerinin hesaplanmasına olumlu yönde katkı sağlar. Denetim risk değerinin kabul edilebilir bir düzeye indirebilmek amacıyla denetçi tarafından mesleki bilgi, tecrübe ve düşüncesini göz önünde bulundurur.

ISA400 göre, **"Denetim Riski"**, finansal tablolarda önemli yanlışlıklar bulunmasına rağmen, denetçinin bu yanlışlıkları tespit edememesi ve bu nedenle yanlış bir görüş vermesi riski olarak tanımlanmaktadır.[58] Tanımlanan risk içerisinde; **doğal risk, kontrol riski ve ortaya çıkarma riski** şeklinde üç alt risk yer almaktadır. Bu riskler;[59]

i) Doğal Risk: İşletme bünyesinde iç kontrol yapısının oluşturulmamasına bağlı olarak, mali tablolarda yer alan hesabın ve/veya işlemin işletme içerisinde karşılaşılacak olan önemli yanlışlıklara ve hatalara karşı olan hassasiyetini ifade eder.

---

57 İBİŞ ve ÇATIKKAŞ, a.g.m., ss.113.

58 Nurten ERDOĞAN, "Muhasebe Denetiminde Niteliksel Önemliliğin Gerekliliği", http://www.journal.mufad.org.tr/attachments/article/435/13.pdf, (25.05.2013), s.3.

59 Semih SOYER, "Uluslararası Denetim Standartları", **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2005, s.97.

ii) Kontrol Riski: İşletme bünyesinde iç kontrol yapısının oluşturulmasına rağmen, mali tablolarda yer alan bir hesaba ve/veya işleme ait bir hatanın-yanlışlığın, işletme içerisinde tespit edilememesi, düzeltilememesi ya da önlenememesi riskini ifade eder.

iii) Ortaya Çıkarma Riski: Denetçi tarafından doğrulama yoluyla gerçekleştirdiği denetim çalışması sonucunda, mali tablolarda yer alan hesaplarda yer alan bir aksaklığın ve/veya yanlışlığın tespit edilememesi riskidir.

İşletme bünyesinde yürütülen faaliyetlerin sonuçları muhasebe sistemi içerisinde muhasebeleştirilir. İşletme bünyesinde yer alan muhasebe sistemi, çeşitli ve sıralı kayıtlardan oluşan bir faaliyet olarak tanımlanmamalıdır. Muhasebe sistemi içerisinde yürütülen faaliyetin hedefi; finansal kayıtların korunması için tanımlanması, bir araya getirilmesi, değerlendirilmesi, hesaplanması, sınıflandırılması, kaydedilmesi, özetlenmesi ve raporlanması gereklidir. İç kontrol sisteminin muhasebe sistemi içerisindeki görevi işletme bünyesinde yürütülen faaliyetlerin düzenli ve verimli bir şekilde gerçekleştirilmesi, işletme varlıklarının korunması, var ise hile ve hataların ortaya çıkartılması ve önlenmesi, muhasebe kayıtlarının tam, doğru ve güvenilir olması sağlanmalıdır. İşletme yönetimi tarafından finansal değerlerin zamanında, tam ve doğru bir şekilde sunulması amacıyla benimsenen politikaların ve işlemlerin uygulanmasını sağlayan mekanizmaya iç kontrol sistemi adı verilir.

İşletme bünyesinde doğal ve kontrol riski birlikte değerlendirildiğinde; denetim faaliyetini gerçekleştiren sorumlu kişiye aşağıdaki belirtilen faydaları sağlar:

i) Finansal tablolarda yer alan ve/veya oluşabilecek olan olası hata ve yanlışlıkların çeşitlerinin belirlenmesi,

ii) Maddi olarak hata ve/veya yanlış işlemlerin gerçekleştirilmesi riskini etkileyen faktörlerin dikkate alınmasına,

iii) İşletme iç kontrol sistemine ve muhasebe sistemine uygun olan denetim işlemlerinin tasarlanmasına,

olanak sağlar.

Teknolojinin gelişmesi ve teknolojinin gelişmesine istinaden işlemlerin daha hızlı ve doğru yapılabilmesi amacıyla işletmelerin operasyonel ihtiyaçlarını karşılayabilmek için oluşturduğu yapıların karmaşıklaşmasına ve birbirleri ile olan ilişkinin artmasına neden olmuştur. Kullanılan sistemlerin ve yürütülen operasyonların çeşitliliği ile bağlantılı olarak işletmelerin ihtiyaçlarının farklılaşması ile birlikte bu durum ortaya çıkmıştır. İşlemlerin karmaşıklaşması, operasyonlar içerisindeki detaya ulaşma isteği ve kullanılan teknolojik alt yapıya olan bağımlılık, işletmeye ait yürütülen finansal işlemlerde hataların oluşmasına neden olabilir. İşletme bünyesinde karşılaşılabilecek olan hatalar işlemleri gerçekleştiren bölüm ve/veya çalışanların dikkatsizliği, tecrübesizliği, bilgisizliği ve yanılması gibi kriterlerden kaynaklanabilir. Finansal işlemlerde ortaya çıkan hatalar mali tabloların güvenilirliğini etkilemekle birlikte, bu hatalara neden olan sebeplerin engellenmesi, etkin bir iç kontrol sisteminin işletmelerde oluşturulmuş olması ile mümkün olabilecektir.

Mali denetim kapsamında, denetim faaliyetinden sorumlu olan denetçinin, denetim çalışmasında karşılaştığı öncelikli problemler muhasebe hata ve hileleridir. Muhasebe hata ve hileleri, genelde, muhasebe kavram ilke ve kurallarına uygun olmayan düzensizlikleri ifade etmektedir.[60]

İşletmeye ait muhasebe sistemi içerisinde yer alan düzensizliklerinin hata ve/veya hile olup olmadığının tespiti kolay olmamakla birlikte ayrımının yapılması amacıyla detaylı çalışmaların yapılması gereklidir. Bunun nedeni; muhasebe sistemi içerisinde gerçekleştirilen hileli işlemler, hatalı yapılan işlemlerin içerisine dahil edilerek saklanmakta ve ortaya çıkarılabilmesi zor işlemlerdir. İşletme içerisinde çalışan personelin gerçekleştirmiş olduğu hataları kasıtlı olarak yapması, hile faktörünün oluşmasına ve ortaya çıkmasına neden olur.[61]

---

[60] Zeynep HATUNOĞLU, Nurettin KOCA ve Mustafa KILLI, "İç Kontrolün Muhasebe Sistemindeki Hata ve Hilelerin Önlenmesindeki Rolü Üzerine Bir Alan Çalışması", **Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt:9, Sayı:20, 2012, s.176.

[61] Hasan TÜREDİ ve Ümmügülsüm ALICI, "Mali Raporlama Hilelerinin Tespit ve Önlenmesinde İç Kontrol Yapısının Önemi", **Finansal Araştırmalar ve Çalışmalar Dergisi**, Cilt:6, Sayı:11, Temmuz 2014, s.121.

İşletme bünyesindeki muhasebe denetiminin öneminin artmasının nedeni, işletme hakkındaki bilgileri kullanan bilgi kullanıcılarının mali tablolara olan güvenlerinin artmasından kaynaklanmaktadır. Bağımsız denetçiler gerçekleştirmiş olduğu denetim çalışmaları kapsamında; işletmenin iç kontrol yapısının incelenmesi konusunu dikkate alır. Bunun nedeni, işletme bünyesinde gerçekleştirilen faaliyetlerin yer aldığı iç kontrol ortamı ve/veya sisteminin sonuçları işletmeye ait mali tabloları oluşturmaktadır.[62]

İşletme bünyesinde yer alan hata ve hilelerin engellenmesi veya asgari bir düzeye çekilmesi iç kontrol yapısının niteliği ile ilgilidir. İç kontrol yapısının etkin bir nitelikte oluşturulması işletmenin finansal verilerinin doğru olmasını sağlar. İç kontrol sistemi kurulması aşamasında muhasebe sistemi içerisindeki hile riskinin tespit edilmesi sağlanmalıdır. Bu durum iç kontrol sisteminin etkililiği için önemlidir. Hile riski, çalışanların içinde bulunduğu işletmenin kaynaklarını ve varlıklarını kasıtlı olarak uygun olmayan bir biçimde kullanarak veya ele geçirerek haksız kazanç sağlamaları olasılığı olarak tanımlanabilir.[63]

1.5 COSO ve Kurumsal Risk Yönetimi

1.5.1 COSO Kurumsal Risk Yönetimi Bütünleşik Çerçevesi

Mevcut durumda işletmeler tarafından farklı iç kontrol yaklaşımları ve sistemler kullanılarak farklı iç kontrol yapılandırmaları meydana getirilmiştir. Bunların bazıları aşağıdaki gibidir:[64]

CobiT (Control Objectives for Information Technology) Modeli: Bu model işletmelerin operasyonel faaliyetlerini yerine getirirken faaliyetlerinde yer alan bilgi sistemleri yazılımlarına ait oluşan ve/veya oluşabilecek olan riskleri kontrol etmek amacıyla oluşturulmuştur. Model, kullanılan bilgi işlem teknolojisi yapısı içerisinde

---

62 Metin ATMACA, "Muhasebe Skandallarının Önlenmesinde İç Kontrol Sisteminin Etkinleştirilmesi", **Afyon Kocatepe Üniversitesi İİBF Dergisi**, Cilt:14, Sayı:1, 2012, s.199.

63 HATUNOĞLU, KOCA ve KILLI, a.g.m., ss.178.

64 ALAGÖZ, a.g.e., s.8.

yürütülen işlemleri de dikkate alarak, iç kontrol sisteminin faaliyet alanını genişleterek bütün işletmeyi kapsam içerisinde değerlendirmektedir. Model içerisinde iç kontrol sisteminin oluşturulması yönetimin sorumluluğunda olduğu belirtilmiştir. İç kontrol sisteminin oluşturulmasına ait sorumluluk görevi; güvenilir finansal raporlama, faaliyet etkinliğini, mevzuata uygunluğu, üretilen bilgilerin tamlığı, doğruluğu ve gizliliğinin sağlaması amacıyla yönetime verilmiştir. İç kontrol sisteminin etkililiğinin sağlanması görevi üst yönetim, iç denetçi ve bağımsız denetçilerin sorumluluğu olarak tanımlanmıştır.

eSAC (Electronic System Assurance and Control) Modeli: Bu model kapsamında oluşturulan sistem e-ticaret uygulamasını kullanan işletmelere yönelik olarak oluşan risklerin ortadan kaldırılması ve/veya minimum seviyeye indirgemeye yönelik olarak oluşturulmuştur. Sistemin amacı, güvenilir finansal raporlamayı, faaliyet etkinliğini ve mevzuata uygunluğu sağlamaktır. Modelin ilgi ve bilgi alanı bilgi işlem teknolojisi üzerinde yoğunlaşır. Oluşturulan sisteme ait kurma ve işletilmesi yönetimin sorumluluğunda olup, kurulan sistemin işletme hedef ve ihtiyaçları doğrultusunda çalıştırılması iç denetim bölümüne aittir.

SysTrust (System Trust) Modeli: Modelin ana hedefi; işletme bünyesinde kullanılan bilgi teknolojileri sistemi içerisinde ortaya çıkan bilgilerin güvenirliğini sağlamaktır. İşletmenin kullanmış olduğu bilgi sistemlerinin oluşturulması yönetilmesi ve gerekli kontrol ortamının oluşturulması işletme yönetiminin, etkili ve verimli bir şekilde faaliyetini sürdürmesi denetçilerin sorumluluğundadır. Model yapısı içerisinde yer alan bilgi sistemleri kapsamı belirlemektedir. Bu modelin kullanılmasının asıl amacı; işletme içerisindeki bilgi güvenirliliği sağlanarak, finansal tabloları ve raporları karar verme ve strateji belirleme aşamasında kullanan yönetimin beklentilerini karşılamaktır.

COSO (Committee of Sponsoring Organizations) Modeli: COSO, Amerikan Sertifikalı Kamu Muhasipleri Enstitüsü (AICPA), Amerikan Muhasebe Birliği (AAA), Finans Yöneticileri Enstitüsü (FEI), Uluslararası İç Denetçiler Enstitüsü (IIA) ve Yönetim Muhasebecileri Enstitüsü (IMA) tarafından oluşturulan bir organizasyondur. COSO tarafından ön görülen ve oluşturulan iç kontrol sistemi içerisinde; işletmenin bütününü kapsayan bir yapı yer almaktadır. Organizasyon tarafından oluşturulan model

içerisinde, işletmeye ait iç kontrol sisteminin oluşturulması ve yönetilmesi işletme üst yönetimine, etkili ve verimli bir şekilde faaliyetini sürdürmesi sorumluluğu ise yöneticilere ait olduğu belirtilmiştir. COSO modeli içerisinde belirtilen iç kontrol kavramının amacı; güvenilir finansal raporlama, faaliyet etkinliğini ve mevzuata uygun bir şekilde işletme faaliyetlerini yürütmektir. Model içerisinde iç kontrol sistemi **sekiz unsurdan** (kontrol ortamı, amaç (hedef) oluşturulması, olayların tanımlanması, risk değerlemesi, riske cevap verme, bilgi ve iletişim, kontrol faaliyetleri, izleme) oluşmaktadır.

Günümüzde yukarıdaki belirtilen iç kontrol yapılandırmalarından uygulamada en fazla kullanılanı COSO ve COBIT uygulamaları olmuştur. COSO tarafından risk kavramı, kurumsal risk yönetimi olarak tanımlanmıştır.

COSO tanıtımı itibariyle kurumsal risk yönetimi, kurumun hedeflerine ulaşması konusunda makul bir güvence sağlamak için tasarlanan bir süreçtir.[65]

Kurumsal Risk Yönetimi (KRY), bir kurumun yönetim kurulu, üst düzey yöneticileri ve diğer çalışanları tarafından şekillendirilen, kurum genelinde ve stratejiler doğrultusunda uygulanan, kurumu etkileyebilecek olası olayların tespit edilmesi ve risklerin, kurumun risk alma isteği kapsamında yönetilmesi için tasarlanan, kurumun hedeflerine ulaşmasını destekleyecek bir süreçtir.[66]

COSO iç kontrol bütünleşik çerçevesi ilk oluşum içerisinde beş ana bileşenden oluşuyordu:

1. Kontrol ortamı,

2. Risk değerlendirmesi,

---

[65] Ebru SÜMER, "Türkiye'de Kamu İç Kontrol Sistemi Kapsamında Hesap Verme Mekanizmaları", **Mesleki Yeterlilik Tezi**, T.C Maliye Bakanlığı Strateji Geliştirme Başkanlığı, 2010, s.23.

[66] T.C Strateji Geliştirme Başkanlığı, "COSO Kurumsal Risk Yönetim Bütünleşik Çerçevesi Ana Metni-Çeviri", http://www.sgb.gov.tr/IcKontrol/KontrolStandartlarYeni/Dokümanlar/Çeviriler/İç Kontrol Bütünleşik Çerçeve-COSO.pdf, (14.10.2011), s.14.

3. Kontrol faaliyetleri,

4. Bilgi ve iletişim ve

5. İzleme

COSO'nun kurumsal risk yönetimi bütünleşik çerçevesi tanımına bağlı olarak, COSO küpü'nün ilk oluşumdan farklı olarak sekiz ayrı bileşeninin olduğu görülmektedir.

Yeni COSO kurumsal risk yönetimi (KRY) çerçevesi işletme genelinde risklerin belirlenmesi ve yönetilmesinin önemini vurgulamaktadır. Kurumsal risk yönetimi bütünleşik çerçevesinde yer alan bu sekiz bileşen;

1. Kontrol ortamı

2. Amaç (hedef) oluşturulması,

3. Faaliyetlerin tanımlaması,

4. Risklerin değerlendirilmesi

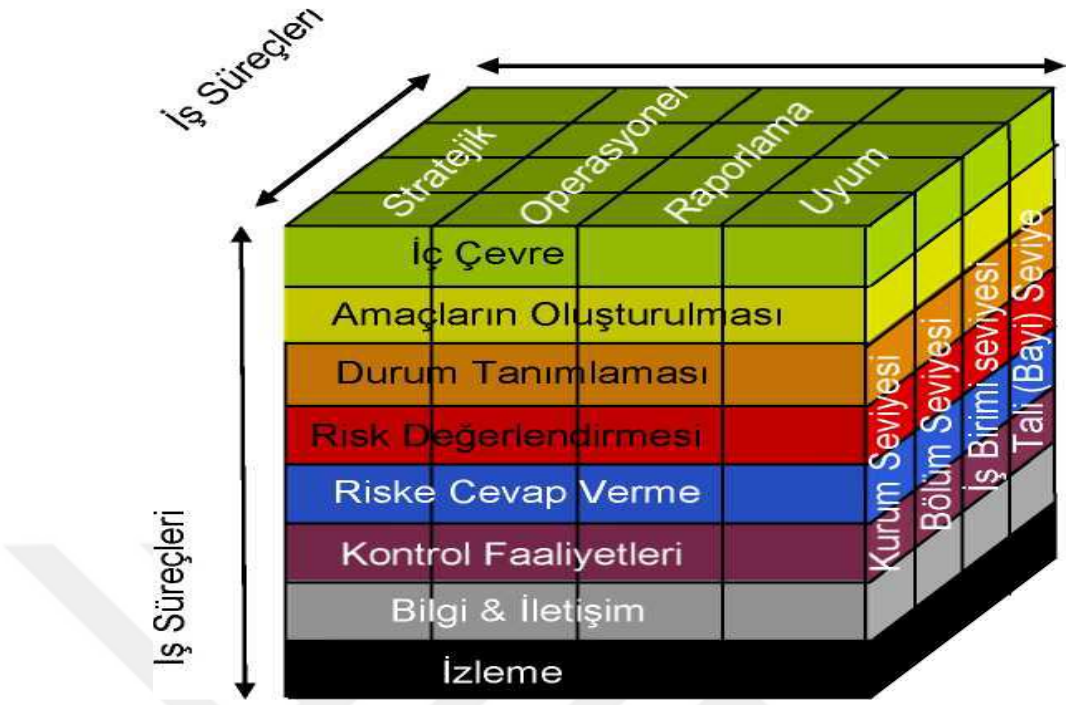
5. Riske cevap verme,

6. Kontrol faaliyetleri

7. Bilgi ve iletişim

8. İzleme

COSO küpü ise kurumsal risk yönetimi çerçevesinde aşağıdaki gibi oluşmuştur.



Şekil 4 : COSO Kurumsal Risk Yönetimi Küpü
Kaynak: Arzu ALİKADIOĞULLARI, "Türkiye'de Mali Reform Kapsamında İç Kontrol Sistemi Uygulaması Maliye Bakanlığı Örneği", **Yüksek Lisans Tezi**, Isparta: Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, 2011, s.42.

Kurumsal risk yönetimi çerçevesinin **üç önemli** bileşeni: "amaçların oluşturulması", "olayların tanımlanması" ve "riske cevap verme"dir.

Yukarıdaki yer alan bileşenlerin detaylı tanımlamaları aşağıdaki başlıklar içerisinde anlatılmaya çalışılmıştır.

1) Kontrol Ortamı: COSO kurumsal risk yönetimi çerçevesine göre kontrol ortamı bir işletmenin yaklaşımını temsil eder.[67] İşletme bünyesinde görev alan çalışanlar tarafından risklerin ne şekilde algılanmasına ve yönlendirilmesi gerektiğine ilişkin bir temel yapı oluşturur. Kontrol ortamı kavramı içerisinde işletme ile ilgili risk yönetimi anlayışı, risk iştahı, dürüstlük, etik değerler ve faaliyet gösterilen çevre gibi kavramlar

[67] COSO Enterprise Risk Managament Integrated Framework - Executive Summary, "Internal Environment – The internal Environment Encompasses The Tone of An Organization", September 2004, s.3.

yer alır.[68] İç kontrol sisteminin ve yapısının başarısında en önemli görev işletme çalışanlarına aittir. Bu nedenle işletmede görev alan her personelin sorumluluk ve yetki alanlarını iyi bilmesi ve uygulaması gereklidir.[69] İşletmenin iç yapısı, diğer kurumsal risk yönetimi unsurlarının tamamı için disiplini ve yapıyı sağlayan bir temeldir. Risk yönetimi işletme içerisinde belirlenen strateji ve hedeflerin, faaliyetlerin yapılanması, risklerin tanımlanması, değerlendirilmesi ve uygulanmasında rol oynar. Risk yönetimi belirtilen fonksiyonları dışında, işletmeye ait kontrol faaliyetlerinin, bilgi ve iletişim sistemlerinin ve izleme faaliyetlerinin tasarım ve işleyişinde görev alır.[70] İşletme içerisinde etkili olmayan bir iç kontrol ortamının işletme bünyesindeki etkisi geniş kapsamlı olabilir. İç kontrol ortamının işletme bünyesinde geniş kapsamlı olarak yer alması, iç kontrol yapısının işletmeyi olumsuz yönde etkileyecek ortaya çıkması muhtemel mali kayıpların yaşanmasına, sektörel imaj ve itibarın etkilenmesine ve başarısızlıkların oluşmasına neden olabilir.[71] İşletme içerisinde görev alan çalışanlara ait görev ve yetki dağılımı, yönetim biçimi, tanımlanmış rol ve sorumluluklar gibi işletme yönetimi ile ilişkili olan unsurlar kontrol ortamı içinde yer alır. COSO uygulama metodu strateji, faaliyet, raporlama ve uyumla ilgili hedefleri içerdiğinden tam olarak bir planlama sürecini ifade eder. Kontrol ortamı kurumsal risk yönetimi yapısının işletme bünyesinde nasıl tasarlanacağı ve işletme bünyesinde ne kadar etkili yerleştirilebileceğine karar verir.

2) Amaç (Hedef) Oluşturulması: İşletmeye ait karşılaşabilecek olan riskler tanımlanmadan önce ilgili risk tanımlamalarından etkilenecek olan işletme hedefleri belirlenir.[72]

İşletme içerisinde belirlenen hedefler üç farklı düzeyde belirlenir. Bunlar stratejik faaliyet düzeyinde, raporlama ve uyumluluk düzeyinde olması beklenir.

---

68 COSO Enterprise Risk Managament Integrated Framework - Executive Summary, a.g.e., s.4.

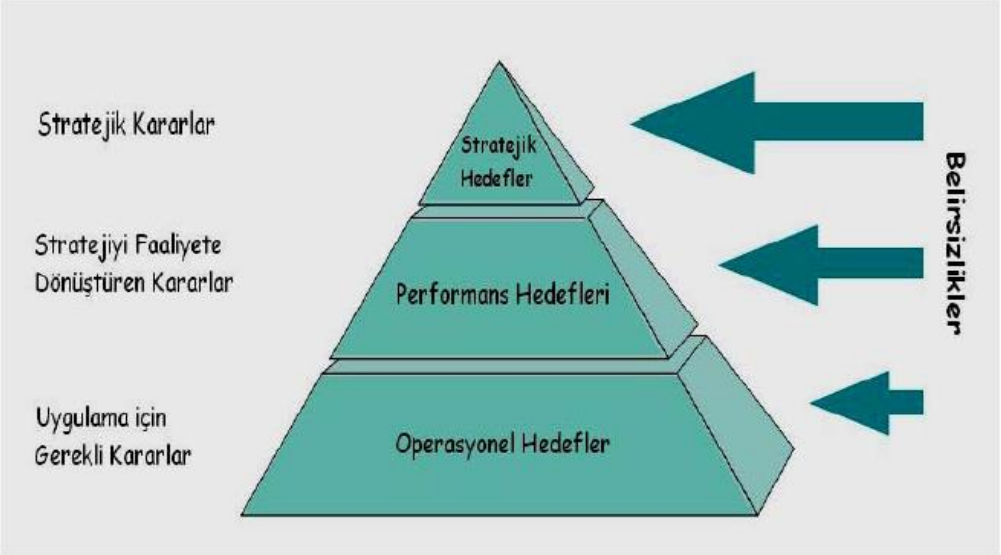
69 Nihat KIRMIZI, "İşletmelerde İç Kontrol Sistemini İncelemenin Bağımsız Denetim Karar Sürecindeki Yeri", **Yüksek Lisans Tezi**, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2007, s.16.

70 İlker TUNÇ, "Kurumsal Risk Yönetim Sisteminin Stratejik Planlamanın Başarısı Üzerindeki Etkisi", **Mali Hizmetler Uzmanlığı Araştırma Raporu**, Yalova, Mart 2014, s.125.

71 T.C Strateji Geliştirme Başkanlığı, a.g.e., s.34.

72 COSO Enterprise Risk Managament Integrated Framework - Executive Summary, a.g.e., s.4.

İşletmeler, işletme bünyesinde ve işletme bünyesinde olmayan dış kaynaklardan kaynaklı olan birçok risk ile karşılaşmaktadır. Bu nedenle işletme içi ve dışı ihtiyaçlara göre etkili ve verimli bir risk tespiti için işletme hedeflerinin belirlenmesi ön koşuldur. İşletme bünyesinde belirlenen hedeflerin işletmeye ait risk iştahı ile paralel bir şekilde belirlenmesi sağlanmalıdır. İşletmeye ait risk iştah seviyesi, işletmeye ait risk seviyelerinde risklerin hangi seviyede olması gerektiğini belirler.[73]



Şekil 5: Hedef Risk Hiyerarşisi
Kaynak: Ebru SÜMER, "Türkiye'de Kamu İç Kontrol Sistemi Kapsamında Hesap Verme Mekanizmaları", **Mesleki Yeterlilik Tezi**, T.C Maliye Bakanlığı Strateji Geliştirme Başkanlığı, 2010, s.26.

İşletme bünyesinde oluşturulan kurumsal risk yönetimi işletmenin vizyonu ve misyonu ile uyumludur. Kurumsal risk yönetimi, işletme stratejilerini ve hedeflerini işletme misyon ve vizyonu ile desteklenmesi amacıyla oluşturulmuştur. Kurumsal risk yönetimi ile uyumlu olan bir strateji faaliyete geçirilirken, işletmenin karşılaşacağı riskleri ve işletmeye ait risk iştahını dikkate alır.[74]

---

73 Hasan TÜREDİ ve Ahmet Oğuz KOBAN, "COSO İç Kontrol Modelinde Risk Değerlendirme Faaliyetleri", **Marmara Üniversitesi Öneri Dergisi**, Cilt:12, Sayı:46, Temmuz 2016, s.174.

74 COSO Enterprise Risk Managament Integrated Framework - Executive Summary, a.g.e., s.4.

COSO kurumsal risk yönetimi bütünleşik çerçevesinde işletme içerisindeki hedef çeşitleri aşağıdaki şekilde oluşturulmuştur.[75] Bu hedefler;

- **Faaliyet Hedefleri:** İşletmenin faaliyetlerinin etkinliği ve verimliliği bu hedef kapsamında değerlendirilmektedir. İşletme faaliyetlerinin işletme hedeflerine bağlı olarak performansı ve verimliliği önemlidir. İşletme hedefleri faaliyetleri kapsamında kayıplara karşı korunma fonksiyonlarını dikkate alarak oluşturulmalıdır. Faaliyet hedefleri, işletme yönetiminin stratejik yapılanma ile ilgili olarak ön gördüğü seçeneklere ve işletme performansına bağlı olarak değişkenlik gösterir.

- **Raporlama Hedefleri:** İşletme faaliyet sonuçlarının raporlanması ve raporlama işleminin güvenirliliği bu hedef kapsamında değerlendirilir. İşletme bünyesinde gerçekleştirilen faaliyetlere bağlı olarak oluşturulan bu raporlar, mali-mali olmayan ve işletme içi-dışı olmak üzere farklı şekilde hazırlanabilir. Hazırlanma çeşidine göre bilgilerin güvenirliği önem teşkil eder.

- **Uyumluluk Hedefleri:** İşletmenin bağlı olduğu kanun ve düzenlemelere paralel olarak işletme faaliyetlerini gerçekleştirmesi bu hedef sınıflandırmasında yer alır. Bu hedef dış faktörlere bağlı olmakla birlikte ve bazı durumlarda tüm işletme bünyesinde, bazı durumlarda ise işletmenin faaliyet göstermiş olduğu tüm sektöre yayılma eğilimi gösterir.

3) Faaliyetlerin Tanımlanması: İşletmelere ait stratejilerin uygulanmasını işletme faaliyetleri etkiler. Bu etki iç ve dış kaynaklardan ortaya çıkan bir durum olup, pozitif ve negatif etkileri birlikte içerisine alır.[76] İşletmenin stratejilerine bağlı hedeflerine ulaşmasını etkileyen iç ve dış faktörler, risk ve fırsatlar dikkate alınarak işletme tarafından tanımlanmalıdır. Ortaya çıkması öngörülen fırsat durumları işletme yönetiminin stratejilerine veya hedef belirleme sürecinde dikkate alınmalıdır.[77] Mevcut durumda işletme içerisinde oluşan ve/veya oluşabilecek olan riskler işletme bünyesinde

---

75 Evren Güncel ERMİSKET, "Kamu Kurumlarında Risk Yönetimi-Bir Uygulama Önerisi", **Kamu İç Denetçileri Derneği Denetişim Dergisi,** Sayı:7, 2011, s.49-50.

76 T.C Strateji Geliştirme Başkanlığı, a.g.e., s.43.

77 T.C Strateji Geliştirme Başkanlığı, a.g.e., s.4.

tanımlanarak, risk farkındalığı oluşturulmalıdır. Farkındalığa bağlı olarak faaliyetlerin tanımlama işlemi, işletme risklerinin etkili bir şekilde yönetilebilmesine olanak sağlar. İşletme yönetiminin tanımlama ve farkındalık oluşturma konusunda bütün iç ve dış faktörleri dikkate almalıdır. İşletmeler bünyesinde oluşturulan risk faktörleri değerlendirildiğinde; işletmeler için risk oluşturabilecek olan dış faktörler aşağıdaki gibidir:[78]

- **Politika:** İşletmenin faaliyetlerini göstermiş olduğu lokasyonlardaki ulusal hükümet ve diğer devlet organlarının etkileri bu kategori içerisinde dikkate alınır.

- **Ekonomi:** Ulusal ve ulusal olmayan piyasalarda gerçekleştirilen işlemler ve bu işlemlerin sonuçlarına bağlı oluşan etkilenmeler işletme için potansiyel ekonomik dış risk alanlarını oluşturmaktadır.

- **Sosyal:** Sosyal faktör işletme dışı bir faktör olarak ortaya çıkabilir. İşletmenin faaliyetlerini sürdürdüğü lokasyonlardaki büyük demografik değişiklik ve sosyal eğilimler işletmenin faaliyetlerini etkiler.

- **Teknoloji:** İşletme dışında, teknolojik gelişmelere bağlı olarak yeni teknoloji kullanımının artması ve buna bağlı olarak işletmenin bu değişimi benimseyip uygulamaması, işletme bünyesinde risk yaratabilir.

İşletmenin risk profilini etkileyen iç faktörler aşağıdaki başlıklardan oluşmaktadır:[79]

- İşletme yönetim ve organizasyonun yapısı,

- Yönetim içerisindeki hesap verme ve sorumluluk yapısı,

- İşletme bünyesinde yer alan değer yargıları, kültürü ve etik anlayışı,

---

78 Sema YİĞİT ve Alperen M. YİĞİT, "Stratejik Yönetimde Dış Çevre Analizi: Kobi'ler ve Büyük İşletmeler Arasında Bir Karşılaştırma", **Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Sayı:38, Haziran-Aralık 2011, s. 122-123.

79 ARSLAN, a.g.e., s.32.

- İşletme operasyonlarının sürdürüldüğü iş çevresi ve tanımı,
- İşletme ve çalışanlara ait risk kültürü ve tolerans seviyesi,
- İşletme bünyesindeki risk yönetimi uzmanlığı ve uygulamaları,
- İşletme içerisinde insan kaynağı yeterliliği ve niteliği,
- İşletme tarafından oluşturulan şeffaflık düzeyi,
- İşletme bünyesinde oluşturulmuş politika, prosedür ve süreçlerin varlığı ve uygulanma düzeyi.

İşletmelerin faaliyet tanımlama işlemi kapsamında, işletme içerisinde çalışanların aktif katılımlarının sağlandığı çalışma ekipleri oluşturulabilir. Faaliyet tanımlama işlemleri geçmiş yaşanan tecrübeleri hem de gelecekte yaşanması muhtemel olayları içerir. Geçmişte yaşanan tecrübeler ödeme tarihçesi, malzeme ve/veya mamul fiyatlarındaki değişim ve zaman kaybı kazaları vb. konuları dikkate alır. Gelecekteki yaşanması muhtemel olaylar ise değişen sosyal ve demografik yapı ve işletmenin içerisinde bulunduğu sektör koşullarını göz önüne alır.[80]

4) Risklerin Değerlendirilmesi: Risk değerlendirmesi, işletme bünyesinde ve/veya işletmenin içerisinde bulunduğu çevre içerisinde oluşan değişiklikleri sürekli olarak takip edip, risklerin tespit ve analiz edilmesi, işletmenin içerisinde bulunduğu iç ve dış pozisyon değişiklikleri ile birlikte oluşan yeni riskleri ortadan kaldırması amacıyla iç kontrol sistemi içerisindeki işletme hedefleri ile uyumlu bir şekilde yapılan değişiklik ve/veya yenileme faaliyetlerini ifade eder.[81]

Risk tanımlaması tamamlandıktan sonra, tanımlanmış olan risklerin işletme yapısı dikkate alınarak, söz konusu risklerin işletmeye olan olası etkilerin ve meydana

---

80 T.C Strateji Geliştirme Başkanlığı, a.g.e., s.45-46.

81 İsmail Fatih CEYLAN ve Mehmet APAN, "Coso İç Kontrol Modeli"nin Yapısal Eşitlik Modeli ile İncelenmesi: Bir Hastane Uygulaması", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt: 6, Sayı:10, Haziran 2014, s.183.

gelme olasılıkları değerlendirilir. Tanımlanan riskler kalıtsal ve artık risk seviyesinde incelenmeli ve değerlendirilmelidir.[82]

Risk değerlendirilmesi yapılırken aşağıdaki belirtilen kriterler dikkate alınmalıdır [83];

- Risk bazında etki ve meydana gelme/gerçekleşme olasılığının net bir şekilde ortaya konulduktan sonra risklerin değerlendirilmesi etki ve meydana gelme/gerçekleşme olasılığı dikkate alınarak tamamlanmalıdır,

- Risk değerlendirmesinin, işletme bünyesinde yer alan bölümlerin çalışma kapsamları ve risk öncelikleri tanımlanarak yapılması,

- İşletmeye ait risklerin kalıtsal risk ve artık risk tabanında değerlendirilmesi gereklidir.

Risk analizi, analiz edilen risk türü, niteliği, analiz hedef, erişilebilen bilgi ve kaynak düzeyine bağlı olarak değişkenlik gösterebilir. Analiz işlemi;

- Kalitatif (niteleyici),

- Yarı-kantitatif (yarı-niceleyici),

- Kantitatif (niceleyici) veya

- Bunların bir birleşimi olan karma

analiz tekniklerinden biri kullanılarak yapılabilir.[84]

İşletme bünyesinde oluşturulan kontrol faaliyetleri risk unsuru göz önünde bulundurularak gerçekleştirilmelidir. İşletme bünyesinde gerçekleştirilen faaliyetlerin ve

---

[82] COSO Enterprise Risk Managament Integrated Framework - Executive Summary, a.g.e., s.4.

[83] ARSLAN, a.g.e., s.34.

[84] Murat BAZIBAŞ, "Operasyonel Risk ve Veri Tabanı Modellemesi", **BDDK Çalışma Raporları**, Mart 2006, http://www.bddk.org.tr/WebSitesi/turkce/Basel/12922006-2.pdf, (11.12.2014), s.20.

kullanılan sistemin bütünüyle güçlü ve zayıf olduğu yanlar değerlendirilerek, riskli olan sahaların tespit edilmesi ve kontrol işlemlerinin söz konusu belirlenen temel alanlarda yoğunlaştırılması gereklidir. İşletme bünyesinde yer alan faaliyetleri ve değişen durumları izleyerek risklerin dinamik olarak tespit edilmesi ve analiz edilmesi amacıyla iç kontrol faaliyetlerinde değişiklik yapılmasına risk değerlendirmesi adı verilir.[85]

5) Riske Cevap Verme: İşletme bünyesindeki risklerin tanımlanıp, değerlendirilmesinden sonra riskler gruplandırılır. Gruplandırılan risk sayısı işletmenin risk kapasitesi ve toleransı ile ilişkili olup olmadığı belirlenir. Gruplanan risk sayısı ile ilgili olarak işletmenin belirlenen risklere karşı oluşturacağı cevabın etkililiği, işletmenin söz konusu risk ile ilgili olarak katlanmayı kabul ettiği risk seviyesi sınırı içinde olmasına bağlıdır.[86] İşletme bünyesinde ortaya çıkan ve/veya çıkabilecek olan risklerin içeriği ve niteliği, söz konusu riskleri kabul etme, kaçınma, azaltma veya paylaşma, şeklinde kategorilerde değerlendirilebilir.[87]

6) Kontrol Faaliyetleri: İşletme tanımlamaları oluşturulduktan sonra risklere verilecek olan cevaplar belirlenir. Bu işlemlerin devamında ise riskleri minimize etmek için yöntemler geliştirme aşamasına geçilir. Kontrol işlemleri, işletme bünyesinde görülmeye devam eden risklerin işletme tarafından ön görülmüş olan risk toleransı ve iştahı kapsamında organize edilmesine, sınıflandırılmasına ve işletmenin yer aldığı sektördeki regülasyonlara uyumunun ve uygunluğun sağlanması amacıyla oluşturulan politika ve prosedürlerden oluşmaktadır.[88]

İşletmenin hedefleri doğrultusunda belirlemiş oldukları amaçlara ulaşmasında risklerin ortaya çıkartılması ve bu risklerle ilgili olarak önlemlerin alınması işletme bünyesinde oluşturulan kontrol faaliyetleri ile gerçekleştirilir.[89]

---

85 İBİŞ ve ÇATIKKAŞ, a.g.m., ss.102.

86 The Orange Book Management of Risk - Principles and Concepts, HM Treasury, Norwich UK 2004, s.27.

87 Şükran GÜNEŞ, "İşletmelerde Hile Riskinin Önlenmesi ve Hastane İşletmelerinde Uygulama", **Yüksek Lisans Tezi**, İşletme Anabilim Dalı, İstanbul, 2014, s.54.

88 COSO Enterprise Risk Managament Integrated Framework - Executive Summary, a.g.e., s.4.

89 T.C Strateji Geliştirme Başkanlığı, a.g.e., s.64.

İşletme bünyesinde oluşturulan politika ve prosedürler kontrol faaliyetlerinin temel yapı taşını oluşturur. Politika; işletme içerisinde belirlenen hedeflere ulaşılması amacıyla hangi faaliyetlerin gerçekleştirilmesini belirlemekte; politikaların yerine getirilmesini ise prosedür sağlar.[90] İşletme organizasyonu içerisinde yer alan kontrol faaliyetleri işletme hedeflerinin oluşmasına güvence sağlar. İşletme organizasyon yapısı içerisinde ve faaliyetlerde hile ve hatanın önlenmesine katkı sağlar. Kontrol işlemleri işletme bünyesinde risk tanımlaması ve değerlendirmesi yapılmış olan risklerin minimize edilmesine katkı sağlar.

İşletme bünyesinde işletmeye özgü olarak oluşturulan politika ve prosedürler işletme yapısındaki tüm fonksiyonlarda geçerli olmalıdır. Politika ve prosedürler işletme bünyesindeki diğer direktiflerin de uygulanmasına yönelik olarak hazırlanır. Politika ve prosedürlerin kapsamı onay mekanizmalarını, sözleşmeleri, performans değerlendirmelerine ait uygun bilgi ve belgelerin ortaya çıkartılmasından ve muhafaza edilmesinden oluşur. Politika ve prosedürlerin kapsamı içerisinde işletmenin bütün temel uygulamaları yer alır. Bu nedenle işletme bünyesinde kontrol faaliyetleri dizayn edilirken, riskleri minimize edebilmek için kontrol faaliyetlerinin sıklığı ve derecesinin tam ve doğru bir şekilde belirlenmesi, işletmenin maruz kalacağı risklerden daha önemli ve riskli bir konudur. Bu nedenle kontrol faaliyetleri oluşturulurken işletme faaliyetlerinin etkinliğini ve verimliliğini etkileyecek olan gereksiz kontrollerden kaçınılmalıdır. Söz konusu bu durumun işletme bünyesinde uygulanmaması, kontrolün etkililiğinin azalmasına ve kontrol faaliyetinin önlemeye çalıştığı riskin ortaya çıkma olasılığını artırabilir.[91]

Kontrol faaliyetleri, riskleri yöneten, yönlendiren ve işletme faaliyetlerinin tam, doğru ve zamanında gerçekleştiğinden emin olmaya yarayan politika ve prosedürün uygulanma alanıdır. Kontrol faaliyetleri, riskleri kabul edilebilir düzeylerde yönetmek için faaliyetlerin içerisinde yer almalı ve kullanılmalıdır.

---

90 Ruveyda KIZILBOĞA ve Filiz ÖZŞAHİN,"Etkin Bir İç Kontrol Sisteminin İç Denetim Faaliyetine ve İç Denetçilere Katkısı", **Niğde Üniversitesi İİBF Dergisi**, Cilt:6, Sayı:2, 2013, s.224.

91 ARSLAN, a.g.e., s.38-39.

İşletme yapısı içerisinde yer alan kontrol ortamında kontrol faaliyetleri dört alanda oluşturulabilir. Bunlar:[92]

- Görevler ayrımı,
- Bilgi işlem süreci,
- Fiziksel kontroller ve
- Performans kontrolleridir.

İşletme içerisindeki kontrol işlemleri mali ve/veya mali olmayan işlemlere ait kontrolleri içermekle birlikte, işletmenin tüm faaliyetleri için bir bütün olarak tasarlanmalı ve uygulanmalıdır. Yetki devri ve onay prosedürleri, görevlerin birbirinden ayrılması, kaynaklara ve resmi kayıtlara erişim konusundaki kontrol işlemleri, kontrol faaliyetlerine örnek olarak gösterilebilir.[93]

7) Bilgi ve İletişim: İhtiyaç duyulan kaynak veri ve bilgiler, işletme içerisindeki faaliyetlerin istenilen süre içerisinde tamamlanması amacıyla belirlenen süre içerisinde tanımlanarak, temin edilir. Temin edilen bilgiler, bilgiyi kullanacak olan kişilere iletilir. İşletme içerisindeki bilgi sistemleri organizasyon içerisindeki bilgi akışının sağlanması amacıyla oluşturulmuştur. İşletme içerisinde üretilen ve/veya dışından temin edilen veri işletme hedeflerine bağlı olarak işletmeye ait risklerin yönetilmesinde kullanılır. İşletme içerisinde etkili bir iletişimin sağlanabilmesi için işletme organizasyondaki iletişim hatlarının karşılıklı olarak oluşturulması sağlanmalıdır. İşletme yönetimi, organizasyon yapısındaki personelin işletmeye ait kurumsal risk yönetimi sorumluluklarının önemini ve içeriğinin anlatılması amacıyla mesaj iletilir. Üst yönetim tarafından gönderilen mesaj çalışanların bireysel olarak göstermiş olduğu faaliyetlerin ve performanslarının, diğer çalışanların yapmış olduğu faaliyetlerle bağlantısını ve işletme içerisindeki kurumsal risk yönetimi içerisindeki rol ve sorumluluklarını benimsemiş olur. Çalışanların işletme bünyesinde kabul edilmiş olan kurumsal risk yönetimi içerisindeki görev ve sorumluluklarını yerine getirebilmesi ve

---

92 Recai AKYEL, "Türkiye'de İç Kontrol Kavramı, Unsurları ve Etkinliğinin Değerlendirilmesi", **Celal Bayar Üniversitesi İİBF Yönetim ve Ekonomi Dergisi**, Cilt:17, Sayı:1, 2010, s.94.

93 CEYLAN ve APAN, a.g.m., ss.183.

yapmış olduğu işlemlere ait bilgilerin bilgi paylaşımını sağlayabilmesi amacıyla yeterli donanımlara sahip olmalıdır. İşletme içerisinde görev alan kişiler işletme bünyesinde içsel iletişim ve dışsal iletişim halinde olurlar. Dışsal olarak gerçekleştirilen iletişimin taraflarına örnek olarak; müşteriler, tedarikçiler ve pay sahipleri verebilir.[94]

İletişim hayatın her alanında önemli bir fonksiyon olmakla birlikte; kurumsal risk yönetimi bileşenlerinden biri olan iletişim kavramı işletmeler için büyük önem taşır. Faaliyetlerin tam, doğru ve zamanında gerçekleştirilmesi amacıyla işletme içerisinde oluşturulan iç kontrol politika ve prosedürlerinin işletme bünyesinde anlaşılması, kabullenilmesi ve sahip çıkılması iletişim aracılığıyla sağlanır. Bu nedenle işletme içerisindeki iletişim yönetiminin tasarlanması ve en iyi şekilde uygulanmasını sağlayacak iletişim kanallarının oluşturulması gereklidir. İletişim yönetimi işletmeden işletmeye farklılık göstermekle birlikte, işletmenin hacmine ve büyüklüğüne bağlı olarak değişkenlik gösterebilir. Bu değişkenlik her işletmede dikkate alınarak iletişim mekanizmaları yazılı ve/veya sözlü olarak oluşturulabilir.[95]

8) İzleme: İşletme bünyesinde oluşturulan kurumsal risk yönetimi çerçevesi ve içeriği periyodik olarak gözden geçirilir ve takip edilir. Kurumsal risk yönetimi sistemine ait genel yapı içerisinde yer alan fonksiyonların verimliliği ve işleyişi analiz edilerek değerlendirilir. Analiz ve değerlendirme işlemi sürekli izleme işlemi ile yerine getirilir. Yapılacak olan değerlendirmenin kapsamını ve periyodunu risklerin değerlendirilmesi ve sürekli izleme uygulamalarının etkililiği belirler. Kurumsal risk yönetimi ile ilgili olarak yapılan izleme işlemine ait tespit edilen hususlar üst yönetime ve yönetim kuruluna hazırlanan rapor ile paylaşılır.[96] İşletme yaşayan bir organizasyon olduğu için işletme içerisindeki kurumsal risk yönetimi zamana bağlı olarak gelişim ve değişim gösterebilir. İşletmenin ihtiyaçlarına bağlı olarak oluşturulan kurumsal risk yönetimi yapısı değişiklik göstermekle birlikte ilk kurulum aşamasında etkili olan risk çözümleri güncel durumda etkisiz bir durum alabilir.[97] İşletme yapısında değişiklikler

---

94 T.C Strateji Geliştirme Başkanlığı, a.g.e., s.72.

95 KIZILBOĞA ve ÖZŞAHİN, a.g.m., ss.225.

96 COSO Kurumsal Risk Yönetim Bütünleşik Çerçevesi Ana Metni, a.g.e., s.81.

97 Sanjay ANAND, **Sarbanes- Oxley Guide for Finance and Information Technology**

dışında; iç kontrol sisteminin kurulum aşamasında tasarlandığı şartlarda değişikliklerin oluşması, yeni kontrol çerçevesinin koşullarına bağlı olarak oluşan risklere karşı olan savunma mekanizmasının yetersiz kalmasına neden olabilir. İşletme içerisindeki bu tür değişikliklerin oluşması durumda, üst yönetim tarafından kurumsal risk yönetiminin mevcut durumda etkili bir şekilde devam etmesini sağlayacak gerekli önlemlerin alınması sağlamalıdır.[98]

Yukarıdaki açıklamalar değerlendirildiğinde; COSO bileşenlerindeki her bir bileşen dört hedefin kesişim bölgesinde yer alır. Örneğin, bilgi ve iletişim bileşeninin bir parçası olan işletme içi ve dışı kaynaklardan üretilen mali ve mali olmayan veriler stratejiyi oluşturmak, işletme faaliyetlerini etkili bir şekilde yönetmek, etkili bir raporlama ve uyulması gereken düzenlemelere uyumluluğun gerçekleştirilmesini sağlar. Bunun yanında hedef bileşeni değerlendirildiğinde, diğer bileşenlerin bileşenler arası olan ilişkisi anlaşılmış olacaktır. Küp içerisindeki bir kategoriyi incelediğimizde; faaliyetlerin etkinliği ve verimliliği açısından küp içerisinde yer alan sekiz bileşenin tamamının uygulanması, işletme faaliyetlerinin etkililiği ve verimliliği, işletme hedefinin gerçekleştirilmesi için gereklidir. [99]

COSO uygulama rehberi 1992 yılında yayınlandıktan sonra, COSO bütünleşik çerçevesi COSO Çerçevesi Komisyonunun ortak kararı ile birlikte Mayıs 2013 tarihinde revize edilmiştir. Yapılan revize kapsamında aşağıdaki belirtilen konularda değişiklikler yapılmıştır:[100]

- İşletme içerisinde yönetim kurulu ve iç denetim komitesinin oluşturduğu etkili ve verimli bir kontrol sisteminin, risk değerlendirme yapısının güçlenmesine bağlı olarak, işletme içerisinde oluşması muhtemel suiistimallerin tespitinde ve önlenmesinde faydasının arttığı belirtilmiştir.

Professionals, John Wiley&Sons, Inc., Vol:2, 2006, s.56.

98 T.C Strateji Geliştirme Başkanlığı, a.g.e., s.82.

99 T.C Strateji Geliştirme Başkanlığı, a.g.e., s.23.

100 Hasan Türedi ve Gencay Karakaya, "COSO İç Kontrol Modeli ve Kontrol Ortamı", **Finans Politik ve Ekonomik Yorumlar Dergisi**, Cilt:52, Sayı:602, 2015, s.70.

- COSO iç kontrol kavramı ve bileşenlerinde önemli bir değişiklik yapılmamıştır.

- Yayınlanan revize kapsamında mali olmayan süreçlerin önemi belirtilmekle birlikte, mali olmayan süreçlerin sürekli izlenmesine ve takip edilmesine yönelik olarak bütünleşik çerçevenin kapsamı genişletilmiştir.

- İşletme içerisinde yapılan iç kontrol faaliyetlerinde, temin edilen ve kullanılan bilginin güvenirliliği ve geçerliliğinin önemi vurgulanmıştır.

- COSO çerçevesinin ana bileşenleri değişmemiş olmakla birlikte, ana bileşenlere ait alt bileşenler içerisine bağlı olsa bile bunların alt bileşenlerine bazı bilgiler dahil edilmiştir. Bunlar;

  - **Kontrol Ortamı:** Bu bileşen içerisinde, üst yönetimin dürüstlük ve etik ilkelere bağımlığından bahsedilmekle birlikte; işletme içerisinde yer alan iç kontrol sisteminin geliştirilmesi, performans yönetimi ve gözetim çalışmalarına yer verilmiştir. İlgili madde kapsamında şirketin iç kontrollerin performansından süreç sahibi ilgili kişileri sorumlu tutacağına yer verilmiştir.

  - **Risklerin Değerlendirilmesi:** İç kontrol sistemlerini etkileyebilecek olayların tanımlanması ve tanımlama kapsamında dolandırıcılık potansiyeli bulunan süreçlerin öngörülmesi gerektiğine yer verilmiştir.

  - **Kontrol Faaliyetleri:** İşletme bünyesinde oluşturulan kontroller, yazılı dokümantasyon yoluyla işletme bünyesinde duyurulur. Oluşturulan kontrollerden ne beklendiği açıkça ifade edilerek, ilgili kontrollerin uygulanması yaygınlaştırılır.

  - **Bilgi ve İletişim:** İşletme organizasyon yapısı içerisinde yer alan iç kontrol faaliyetlerini etkileyen hususların tespit edilmesi durumunda ilgili taraflarla iletişim kurulur. Kontrollerin etkin ve verimli bir şekilde devam etmesi için organizasyon içi, dışı bilgi iletişiminin sürekli olması sağlanır.

- **İzleme:** Kontrol yapısına ait tespit edilen kontrol eksiklikleri düzeltilmesinden sorumlu olan kişiler dahil olmak üzere üst yönetim ve yönetim kuruluna zamanında bildirilir ve gerekli alınacak olan aksiyonlar takip edilir.

Kurumsal risk yönetimi; organizasyonların büyüklüğünü ve misyonlarını gözetmeksizin olayların tanımlanmasını sağlar. Kurumsal risk yönetimi işletme stratejik hedefleri, projeleri, girişimleri ve günlük uygulamaları zorlaştıran risk unsurlarının işletme bazında, birbirleriyle iletişimlerini gözetir. İşletmenin faaliyetlerini uygulama aşamasında karşılaşılan risklerin önceden belirlenip, değerlendirilmesine olanak sağlar. Belirlenen riskler kurumsal risk yönetimi tarafından en verimli bir şekilde işletme içerisinde yönetilmesine yardımcı olur. İşletmenin faaliyetlerine bağlı olarak ortaya çıkabilecek olan belirsizliklerin değerlendirilmesinde ve yönetilmesinde kurumsal risk yönetimi görev alır. Bu görevi strateji, süreç, çalışanlar, teknoloji ve bilginin birbirleriyle uyumunu sağlayacak bir şekilde yerine getirir.[101]

COSO tarafından tanımlanan kurumsal risk yönetimi aşağıdaki belirtilen kavramları içermekle birlikte, söz konusu kavramları birleştirdiğimizde; risk yönetimi kapsamında aşağıdaki tabloda belirtilen şekilde bir iş akış süreci ortaya çıkmaktadır.[102]

---

[101] Pricewaterhousecoopers, "Kurumsal Risk Yönetimi Temel Kavramlar ve Uygulamalar", 2007, https://www.vergiportali.com/doc/fuar2007/kurumsalriskyonetimi.pdf, (12.03.2010), s.6.

[102] Erdal DURAN, "Kamu İdarelerinde Kurumsal Risk Yönetimi Uygulamaları", **Mali Hizmetler Uzmanlığı Araştırma Raporu**, Ankara, 2013, s.32.

Şekil 6: COSO Kurumsal Risk Yönetimi Süreci İş Akışı
Kaynak: Maliye Bakanlığı Strateji Geliştirme Daire Başkanlığı, "Kurumsal Risk Yönetimi Dokümanı", Mart 2008, s.40.

Risk yönetim faaliyetinin amacı; işletmelere bünyesinde taşıdıkları risklerle uyumlu sermaye tahsisinin sağlanması, korunması ve risk faktörü dikkate alınarak oluşturulan sermaye getirisini en üst düzeye çıkartarak işletmeye katma değer artışını

sağlamaktır. Risk yönetiminin diğer önemli hedefi, işletme içinde veya dışında yer alan karar alma yapıları için riskleri ortaya çıkarabilir ve ölçümlenebilir bir format haline getirerek işletmelerin çok yönlü hareket kabiliyetlerinin artışını sağlamaktır.[103]

Risk yönetim kavramı bir yöntem olarak değerlendirildiğinde, işletme organizasyonlarının periyodik olarak belirledikleri ve değerlendirdikleri risk çeşitlerine, aktiviteler ekleyerek eklenen aktivitelerin hedeflere ulaşmalarını destekler.[104]

İşletme içerisinde iyi bir risk yönetimi; riskleri belirleyen ve belirlenen bu risklerin değişikliklerini ön planda tutan bir yönetim anlayışıdır. Risk yönetimi, organizasyon yapısı içerisinde yer alan bütün faaliyetlere en yüksek düzeyde ve seviyede değer katmayı hedefler. Risk yönetimi, işletme içerisindeki kontrol ortamını ve organizasyon yapısını etkileyen potansiyel bütün unsurları değerlendirir ve işletme için ne ifade ettiğini tanımlar. İşletmeye ait başarı ve başarısızlık durumu, risk yönetiminin hedeflere ulaşma sırasında ortaya çıkabilecek olan belirsizlikleri minimize etmesine bağlıdır.

Risk yönetimi süreci işletme içerisinde aşağıdaki belirtilen temel hedeflere odaklanır;

1. İşletme stratejilerine bağlı olarak gerçekleştirilen faaliyetlerden kaynaklanan risklerin belirlenmesi, tanımlanması ve önem düzeyine göre önceliklendirme işleminin yapılması,

2. Yönetimin, denetim komitesinin ve yönetim kurulunun, işletmenin stratejik planlarının gerçekleştirilmesi amacına yönelik risk kabulünü dahil ederek, işletmenin kabul edebileceği risk seviyelerinin belirlenmesi,

3. Belirlenen riskleri, üst yönetiminin belirlediği kabul edilebilir risk seviyelerine indirilmesi veya başka belirlenen yöntemlerle risk seviyelerinin

---

[103] BAŞARIR, a.g.e., s.7.

[104] AIRMIC (The Association of Insurance and Risk Managers), "**A Risk Management Standard"**, 2002, s.2.

düşürülmesine yönelik alınacak aksiyon ve faaliyetlerin organize edilmesi ve uygulamaya geçilmesi,

4. Riskleri ve risk yönetimi amacına yönelik kontrollerin etkinliğini dönemsel olarak yeniden değerlendirmek için, sürekli izleme faaliyetlerinin yürütülmesi,

5. Risk yönetimi süreçlerinin sonuçları hakkında, yönetime ve yönetim kuruluna dönemsel olarak raporlama yapılarak, işletmenin kurumsal yönetim süreçleri kapsamında; riskler, risk stratejileri ve kontrolleri hakkında hissedarlara ve diğer hak sahiplerine dönemsel bilgi verilmesidir.

Risk yönetimi organizasyon stratejileri ve bu stratejilerin değişkenliği ile uyumlu bir şekilde hareket etmeli ve sürekli olarak gelişim göstermelidir. Risk yönetimi geçmiş, gelecek ve mevcut durumdaki uygulanan organizasyonu saran risklerin belirlenmesi yönünde çalışma yapar. İşletme bünyesinde risk yönetimi en üst kademeden en alt kademeye kadar işletmenin bütün yapısı içerisinde, işletme kültürüne sürekli gelişim gösterecek şekilde dahil edilmelidir. Risk yönetimi işletmenin stratejisini taktiksel ve operasyonel hedeflere çevirmelidir. İşletme stratejisini taktiksel ve operasyonel hedeflere çevirirken, her bir yöneticiye ve çalışanın organizasyondaki sorumluluklarını ayırarak, görev tanımlarında yer alan risk yönetimi kısımlarını belirleyerek yapmalıdır. Bu durum performans ölçümünü, sorumluluğu ve ödüllendirmeyi desteklemekle birlikte, operasyonel efektifliği bütünsel anlamda artırmaktadır.

Risk yönetimi bir yönetim aracı olup, bu araç organizasyonun arzu ettiği risk/kazanç dengesine ulaşılabilmesi amacıyla kullanılmaktadır. Risk yönetimi işletme içerisindeki bir ürünün planlanması, araştırma geliştirme faaliyetlerinden başlamakta, ilgili ürünün müşteriye sunulmasından sonra devam eden müşteri ilişkileri yönetimi aşamasına kadar tüm aşamaları değerlendirir. Değerlendirme sonucunda gerçekleştirilen veya gerçekleştirilmesi planlanan bütün fonksiyonlara yer verir. Risk yönetimi bir işletme içerisindeki yer alan her faaliyetle ilgi süreçlerin tamamını çalışma kapsamına dahil eder. İşletmenin bütününde yer alan faaliyetleri kapsaması nedeniyle risk yönetimi, bu faaliyetleri gerçekleştiren bütün işletme çalışanlarını da içerir. Çalışanları da kapsayan ve

yakından ilgilendiren risk yönetimi kavramı, çalışanlarla paylaşılmalı ve bu kavramla ilgili olmaları ve faaliyetlerini yürütmeleri sağlanmalıdır.

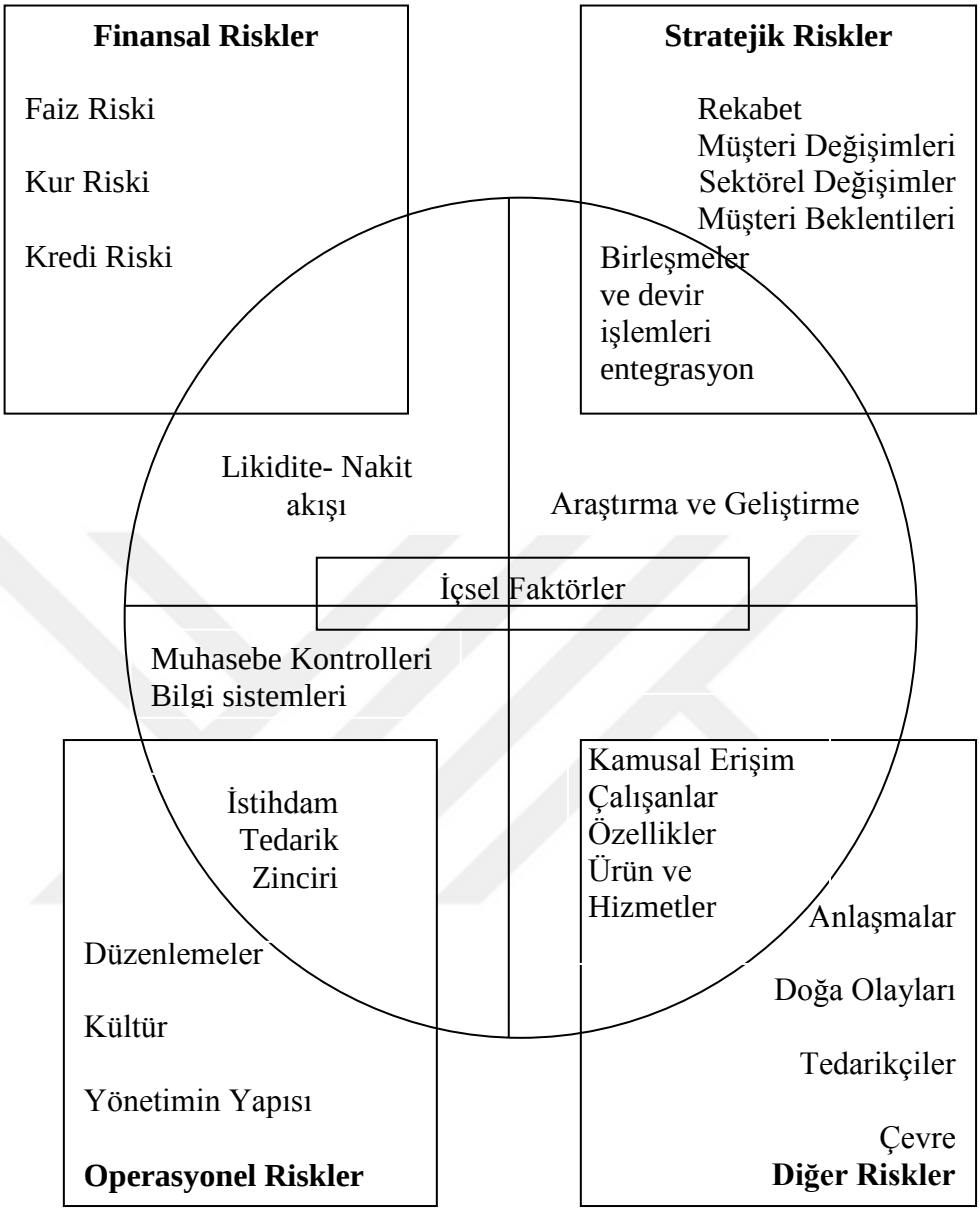
Risk yönetimi işletmeye ait risklerin belirlenmesi, üst yönetimin risk iştahına göre risk önceliklerinin yapılması ve risk önceliğine göre öncelikli olarak minimize edilecek olan risklerin değerlendirildiği, belirlenen risklerin yönetilmesi amacıyla strateji ve planların geliştirilip uygulandığı sistematik ve dinamik bir süreci ifade eder.

1.5.2 Anahtar ve Performans Risk Göstergeleri

Riskler, organizasyon yapısını bir katman olarak çevrelemektedir. Organizasyondaki iç ve dış faktörlerin her ikisi de risk faaliyetlerinin sonuçları olabilir. Aşağıdaki belirtilen şekil içerisinde, anahtar riskler özetlenmiş ve bazı spesifik risklerin iç ve dış faktörlere sahip olduğu gösterilmiştir. Riskleri çeşitli sınıflamalara ayırmak mümkün olup, bunlar stratejik, finansal ve operasyonel riskler vb. olarak sıralanabilir.

İşletmeler varlığını sürdürdüğü sürece birden fazla çeşitli risk faktörleri ile karşılaşmaktadır. İşletmeler için önemli olan karşılaştıkları risk faktörlerini ne şekilde ve nasıl yöneteceğidir. Risk yönetimi kavramı işletmelere bu noktada yardımcı olarak riskleri minimize etmelerini sağlar.

Şekil 7 içerisinde belirtilen anahtar risk faktörleri ile birlikte işletme bünyesine işletmeye özgü olarak belirlenen anahtar performans göstergeleri (APG-KPI: Key performance indicators) ve işletmeye ait anahtar risk göstergeleri (ARG-KRI: Key risk indicators) şekil içerisinde belirtilmiş olan anahtar risk faktörlerinden en az seviyede etkilenmesini sağlayacaktır.



Şekil 7: Anahtar Risk Faktörleri
Kaynak: AIRMIC (The Association of Insurance and Risk Managers), **A Risk Management Standard**, AIRMIC, 2002, s.3.

Anahtar risk göstergesi, potansiyel bir riskin varlığı, düzeyi ve trendi hakkında bilgi veren bir ölçüm aracı olarak tanımlanmaktadır. Oluşan ve/veya oluşma olasılığı yüksek olan bir risk çeşidi veya ortaya çıkma olasılığı olan diğer bir risk çeşidinin de tespit edilmesini anahtar risk göstergesi sağlayabilir. Bu göstergenin ve/veya işaretin oluşması işletme içerisinde **"erken uyarı"** yapısının oluşmasını sağlayarak, işletme üst yönetimine ve yöneticilere potansiyel risk ile ilgili olarak riski karşılayıcı yönde

önlemlerin alınmasına olanak sağlayabilir. İşletme bünyesinde, yürütülen faaliyetler bazında anahtar risk göstergelerinin tanımlanması, oluşturulması ve izlenmesi büyük önem taşır. İşletme bünyesinde anahtar risk göstergelerinin izlenmesi, işletme içerisindeki faaliyetlerin işletme hedefleri ile uyumlu bir şekilde gerçekleştirilip, gerçekleştirilmediğinin değerlendirilmesini sağlar. Anahtar risk göstergesi işletme bünyesinde risk profilinin güncel olarak oluşturulmasına ve erken uyarı mekanizmalarının kurulmasına olanak sağlar.[105]

İşletmenin stratejik seviyedeki faaliyetlerinin performanslarını değerlendirmek ve işletme bünyesinde verimliliği sağlamak amacıyla oluşturulan ve kullanılan ölçüm göstergeleri anahtar risk göstergesi olarak tanımlanmaktadır. Anahtar risk göstergeleri ve anahtar performans göstergeleri işletme bünyesinde aynı hedef doğrultusunda uygulanmaktadır. İşletmenin performans hedefleri ile ilişkili olan anahtar performans göstergeleridir. İşletme bünyesindeki faaliyetlere ait performanslarının ölçülmesinde anahtar performans göstergeleri kullanılır. Anahtar performans göstergeleri "geçmişe yönelik" bir değerlendirme ve analizi işaret eder.

İşletme bünyesinde belirlenen risk seviyesine işletme içerisinde ne kadar düzeyde yakınlaşıp, yakınlaşılmadığı konusunda anahtar risk göstergesi bilgi verir. İşletme bünyesinde tanımlanan risk ve risk çeşitlerinin meydana gelme ihtimali ve işletme bünyesindeki etkisi anahtar risk göstergeleri ile değerlendirilip, izlenebilir. İşletme bünyesinde belirlenen risk seviyeleri; anahtar risk göstergesi ile performansını etkileyecek olan faktörlerin önceden belirlenmesinde belirleyici bir fonksiyon olarak ortaya çıkar. İşletme bünyesinde anahtar performans ve risk göstergelerine ait risk seviyelerinin tam, doğru ve zamanında belirlenmesi önemlidir.[106]

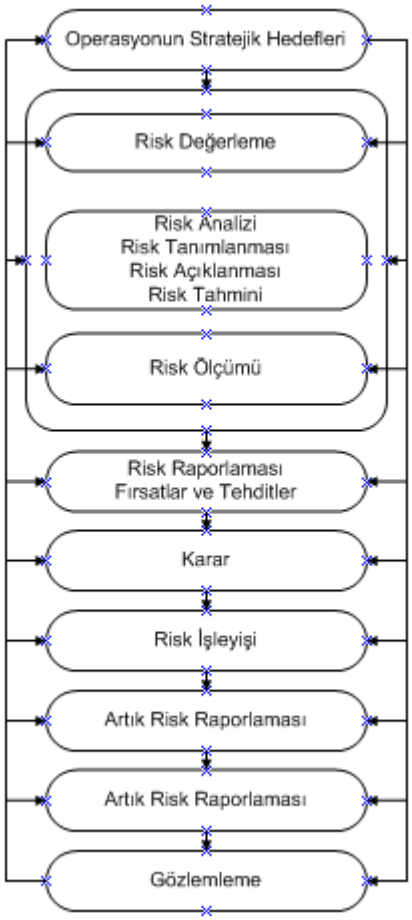
Yukarıdaki belirtilen tanımlamalardan anlaşılacağı gibi anahtar performans göstergeleri geçmişe dönük, anahtar risk göstergeleri ise "geleceğe dönük" erken uyarı mekanizmalarıdır. (örn. Suiistimale konu olan personel vaka sayısı-**Anahtar**

[105] Aravind IMMANENI, Chris MASTRO ve Michael HAUBENSTOCK, "A Structured Approach to Building Predictive Key Risk Indicators", **Operational Risk: A Special Edition of The RMA Journal**, May 2004, Sayı: 42-43.

[106] KAHYAOĞLU, a.g.e., s.45.

Performans Göstergesi, Yıllık izin kullanmayan personel yüzdesi- **Anahtar Risk Göstergesi-** Kasa açıklarına neden olan personel bilgisi-**Anahtar Performans Göstergesi,** Kasa açıklarının artması-**Anahtar Risk Göstergesi,** Banka çalışanın muhasebe sistemi içerisinde oluşturduğu muhasebe belgesi fişlerine ait iptal işlemlerinin artması- **Anahtar Risk Göstergesi**)

Anahtar risk göstergeleri ve işletmenin faaliyetleri bir bütün olarak değerlendirildiğinde aşağıdaki belirtilen süreç akışı ortaya çıkmaktadır.



Şekil 8: Risk Yönetimi Süreci
Kaynak: AIRMIC (The Association of Insurance and Risk Managers), **A Risk Management Standard**, AIRMIC, 2002, s.4.

İşletme bünyesindeki risk yönetimi; organizasyonu ve organizasyonun pay sahiplerini koruyarak ve organizasyona değer katarak, organizasyonun hedeflerini şu şekilde destekler;

a) Taslak bir çerçeve oluşturarak, organizasyonun gelecekteki aktivitelerini uyumlu ve kontrollü bir biçimde gerçekleştirmesini sağlamak,

b) Organizasyonun iş faaliyetlerini ve projeye ait fırsat ve tehditleri algılayarak, bu konular hakkında hangisi için daha öncelikli olarak karar alınmasını, planlamasını ve öncelik verilecek olan işlem ve faaliyetlerin belirlenmesini sağlamak,

c) Kaynakların ve sermayenin organizasyon içerisinde etkin bir şekilde dağıtılmasını ve tahsis edilmesini sağlamak,

d) Asıl faaliyet konusu dışında faaliyet gösterilen alanlarda değişkenliğin ve belirsizliğin azalmasını sağlamak,

e) Kurum imajını ve varlıklarını korumak ve geliştirmek,

f) Operasyonel efektifliği optimize etmektir.

2. BÖLÜM
BANKACILIK SEKTÖRÜNDEKİ RİSK SINIFLAMALARI VE RİSK YÖNETİMİ KAVRAMI

2.1 Bankacılıkta Risk Kavramı

İşletmelerin karşılaştıkları risk çeşitlerini değişik şekillerde sınıflandırmak mümkündür. İşletmenin yer aldığı sektör ve organizasyonel özellikleri işletmenin karşılaşabileceği risk özelliklerini ve sınıflandırmayı etkilemektedir. Riskleri temelde 4 başlık altında sınıflandırmak mümkündür. Bunlar; finansal, operasyonel, stratejik ve dış çevre riskleridir. Bu risk sınıflandırmaları birbirleriyle yakından ilişkisi olan ve birbirinden ayırmanın pek mümkün olmadığı risklerdir. Örneğin; işletmeye ait oluşan kredi riskine ait bir durumun neden ve sonuçları değerlendirildiğinde; sonuçları finansal riskleri, nedenleri ise operasyonel riskler olarak ortaya çıkabilir.

Finansal Risk: İşletmenin içerisinde bulunduğu finansal duruma bağlı olarak seçtiği ve/veya tercih ettiği finansal çözümleri sonucunda ortaya çıkan riskler finansal risk olarak tanımlanır. İşletme bünyesinde finansal risk tanımı içerisinde kredi, faiz, nakit, finansal piyasalar, emtia fiyatları gibi riskler dikkate alınır. İşletmelerin karşılaştıkları riskleri, "finansal riskler" ve "finansal olmayan riskler" iki gruba ayrılabilir. Finansal olmayan olarak tanımlanan riskler, işletmenin faaliyet göstermiş olduğu sektör içerisinde, faaliyet sonuçlarına bağlı olarak karşılaştıkları ve işletme içerisinde görev alan yöneticilerinin sektör tecrübesi, problem çözme yetenekleri, işin bütünü dikkate alabilen özellikleri sayesinde önleyebilecekleri türde riskleri ifade eder. Bu türdeki bir risk tanımına örnek verilmek istenirse; üretim işlemlerinde ortaya çıkan sorunlar ve/Veya aksaklıklar, kullanılan teknolojik alt yapının mevcut koşullardaki gereksinimleri yerine getirememesi, sektör içerisinde yer alan diğer işletmelere ait ürünlerin sektör içerisinde kendilerini ön plana atması; gibi pek çok örnek bu tür riskler için verilebilir. Bu tür risklerin işletmeye mutlaka bir finansal etkisi olmaktadır. Ancak risk durumunun tam

olarak ortadan kaldırılması, bütünüyle işletmenin yönetim gücüne ve becerisine bağlı olarak değişkenlik göstermektedir. [107]

Operasyonel Risk: İşletmenin faaliyetlerini etkin ve verimli bir şekilde yerine getirme aşamasında karşılaştığı engellemeler, yetersiz ve/veya başarısız iş süreçleri, işletme çalışanlarından ve işletmenin faaliyetlerini yürüttüğü sistemlerden veya işletme dışındaki ve kontrolündeki durumlardan kaynaklanan ve yasal riski türünü de bünyesinde barındıran, zarar etme olasılığı operasyonel risk olarak ifade edilmektedir. Bu tanımlamaya bağlı olarak çalışan hataları, kullanılan sistem içerisindeki oluşan hatalar, iş süreçlerindeki aksaklıklar-verimsizlikler ve işletme dışı faktörler operasyonel riskin 4 temel nedenidir.[108] Satın alma, ürün geliştirme, satış ve müşteri ilişkileri yönetimi gibi risk çeşitleri bu kategori içerisinde değerlendirilmesi gereken risk çeşitlerindendir.

Operasyonel risk, işletmenin, işlemlerin etkinliği ve verimliliği, varlıkların korunması ve bütünlüğü sağlamaya yönelik risklerin belirlenmesi ve yönetilmesinde başarısız olması ve dolayısıyla hedeflerini gerçekleştirememesi durumunda ortaya çıkar.[109]

Stratejik Risk: İşletmeler üst yönetimin belirlemiş olduğu hedef ve stratejiler kapsamında faaliyetlerini planlar. Bu aşama kapsamında işletmeler risklerini kısa, orta veya uzun vadelerde belirleyebilir. İşletmenin söz konusu belirlemiş olduğu hedeflere ulaşmasını engelleyebilecek olan yapısal riskler stratejik risk olarak tanımlanır.[110]

Dış Çevre Riskleri: İşletme faaliyetlerinde bağlı olmayan ancak risk olarak ortaya çıkan, işletmenin faaliyetlerinde tercihlere göre işletmeyi etkileyen risklere dış

---

[107] Berk ÇAĞDAŞ ve Cudi Tuncer GÜRSOY, "Şirketlerde Finansal Risk Yönetimi Amaçlı Bir Modelin Geliştirilmesi Yöntem ve Aşamaları", **İTÜ Dergisi**, Cilt:2, Sayı:3, Haziran 2003, s.56.

[108] Mehmet Ali CANDOĞAN ve Mikail ALTAN, "Basel Kriterleri Çerçevesinde Operasyonel Risk Ölçüm Yöntemlerinin Karşılaştırılması: Örnek Bir Uygulama", **Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Sayı:31, 2014, s.268.

[109] Beliz KORKUT, "Merkez Bankalarında İç Kontrol ve Risk Ölçümü Uygulamalarının TCMB Kambiyo Muhasebesi İşlemleri Açısından Değerlendirilmesi", **Uzmanlık Tezi**, TCMB Muhasebe Genel Müdürlüğü, Şubat 2004, s.45.

[110] KORKUT, a.g.e., s.45.

çevre riskleri adı verilir. İşletmenin içerisinde bulunduğu ortama ait oluşabilecek olan riskler; sektördeki, regülasyonlardaki ve müşteri eğilimlerindeki değişiklikler bu tür risk kategorisinde yer alan risklere örnek olarak verilebilir.[111]

Aşağıdaki şekil içerisinde tanımlaması yapılan risklere ait örnek bir risk modeli yer almaktadır:

[111] KORKUT, a.g.e., s.45.

<table>
<tr><td colspan="2">Finansal Riskler</td><td colspan="3">Operasyonel Riskler</td></tr>
<tr><td>Piyasa
Faiz
Kur
Türev Enstrümanlar
Fiyat</td><td>Kredi ve Likidite
Borcunu Ödeyememe
Teminat
İş Tarafları
Ödeme
Yatırım yenilenmesi
Nakit transferi</td><td>İş Operasyonları
Müşteri memnuniyeti
Ürün geliştirme
Verimlilik
Kapasite
Ürün Çevrimi
Performans
Kaynak</td><td colspan="2">Fiyatlama
Zamanının dolması
Uygunluk
İş kesilmesi
Ürün/Servis Kesintisi
Çevre Etkileri
Sahtekarlık</td></tr>
<tr><td>Sermaye Yapısı
Sermaye
Borç
Varlık/Borç Dengesi</td><td>Finansal Raporlama</td><td>Teknoloji
Gizlilik
Bütünlülük
Erişebilirlik
İlgili bilgi</td><td>Varlık
Fiziksel
Marka Bozulması
Veri
Bilgi
Saygınlık</td><td>Kurum Kültürü
İnsan Kaynakları
Eğitim</td></tr>
<tr><td colspan="5">Stratejik Riskler</td></tr>
<tr><td colspan="2">Piyasa Şartları
Rekabet
Hassaslık
Sermaye yeterliliği
Sektörel
Finansal Piyasalar
Derecelendirme Kuruluşları
Reasürans</td><td>Yönetim
Liderlik
Otorite
Limitler
Dış kaynak
Hedef belirleme
İletişim</td><td colspan="2">Paydaşlarla ilişkiler
Hissedarlar
İş ortakları
Müşteriler
Devlet
Tedarikçiler</td></tr>
<tr><td colspan="5">Dış Çevre Riskleri</td></tr>
<tr><td>Hukuksal</td><td>Politik</td><td>Düzenleme</td><td colspan="2">Felaket</td></tr>
</table>

Şekil 9: Örnek Risk Modeli

Yukarıdaki şekil içerisinde yer alan risk çeşitleri incelendiğinde, risk çeşitlerini birbirinden kesin çizgilerle ayırmak çok zor olduğu ortaya çıkmaktadır.

Finans kurumları içerisinde önemli yeri olan bankalar için risklerin ve risk çeşitlerinin özel bir yeri bulunmaktadır. Bankaların temel faaliyeti finansal aracılıktır. Finansal aracılığın temelinde ve doğasında başka işletmelerin üstlenmek istemediği kredi, likidite ve faiz gibi riskleri üstlenmesi yer alır. Bu işlemi bankalar gerçekleştirebilmek için belirsizliği azaltacak yönde hizmetler sunar. Bankalar diğer işletmelerden farklı olarak, risk alır, yönetir ve bu özelliklerini servis olarak müşterilere sunarlar. Risk alınma işlemi bankalar tarafından iyi yönetilememesi durumunda yok oluşuna neden olabilir.[112] Faaliyet gösterilen alanlarda risklerin olmadığı bir çevrede bankalara ihtiyaç duyulmayacağı açıktır. Bu bakımdan bankalar **"riskin yönetilmesi faaliyeti"ni** gerçekleştirir. Bankalar risk yönetim faaliyetini, üstlendiği riskleri en aza indirerek, risk ve belirsizlikten sağladığı faydayı ise en fazla artırmaya çalışarak yerine getirmeye çalışırlar.

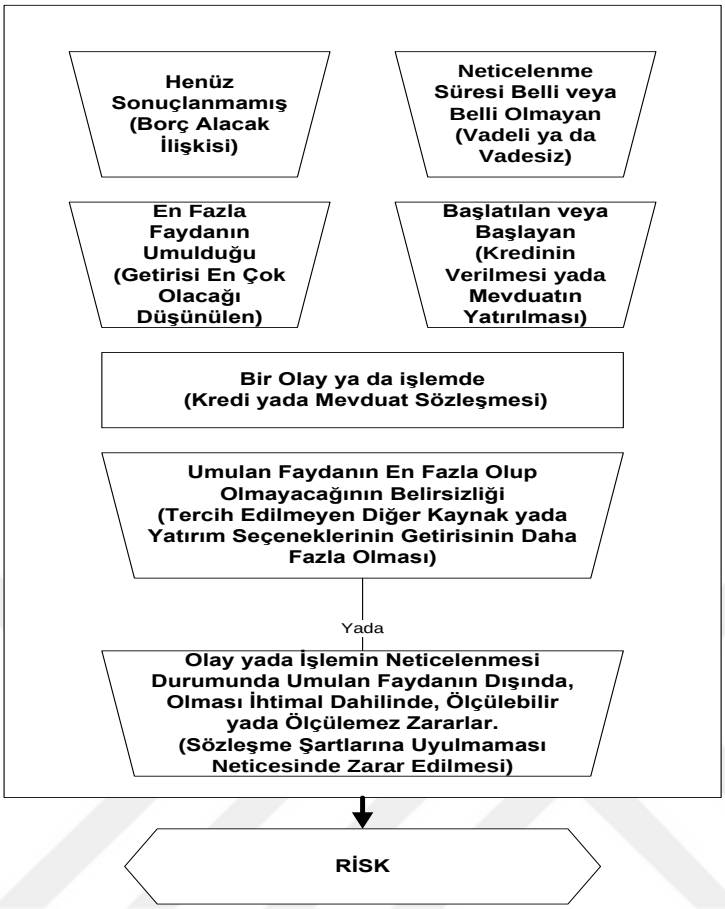
Bankalar kaydi para yaratma fonksiyonuna sahip olmakla birlikte esas faaliyeti bir müşterinin parasını diğer bir müşteriye kullandırmaktır. Bu fonksiyon dikkate alındığında, bankaların pasiflerine oranla öz kaynak miktarları çok küçüktür. Bunun yanında pasiflerin çoğunu oluşturan mevduat kalemleri, talep edildiğinde ödenmek zorundadır. Ancak bankanın aktiflerini oluşturan krediler, vadesinden önce geri çağrılması ve tahsilatının gerçekleştirilmesi mevduat ödemeleri ile karşılaştırıldığında kolay olmamaktadır. Bu nedenle bankaların gerçekleştirmiş oldukları finansal aracılık faaliyeti, bankaların değişken ve kaygan bir zeminde faaliyet göstermesine neden olmaktadır.

Bir işletme olarak bankaların teorik bir yaklaşımla risk terimine maruz kaldığı ve kullandığı şartlara bakıldığında aşağıdaki tabloda yer alan sıralama ile karşılaşılır:[113]

---

[112] Active ARAŞTIRMA, "Bankalarda Performans ve Risk Yönetimi: Analitik bir Çerçeve", **Active Bankacılık ve Finans Dergisi**, Sayı:15, Ekim-Kasım 2000, s.6.

[113] Ferhat SAYIM ve Selami ER; "Risk Kavramı ve Bankacılıkta Risk"**, TMSF Çatı Dergisi**, Sayı:22, Temmuz-Ağustos-Eylül 2009, s.11.



Şekil 10: Bankacılıkta Risk Teriminin Kullanım Aşamaları
Kaynak: Ferhat SAYIM ve Selami ER; "Risk Kavramı ve Bankacılıkta Risk"**, TMSF Çatı Dergisi**, Sayı:22, Temmuz-Ağustos-Eylül 2009, s.12.

Yukarıdaki şekil içerisindeki bilgiler değerlendirildiğinde; bankalar esas olarak risk alan ve satan işletmeler olarak tanımlanabilir. Bankalar bu özelliğinin yanında, bankaların diğer işletmelerden ayrıldığı başka yönlerde bulunmaktadır. Bankaların kendilerine özgü çalışma alanları ve regülasyona tabi oldukları alanlar bulunmaktadır. Bankalar yer aldığı sektöre özgü çalışma koşullarının yanında; diğer işletmeler gibi aynı kanun ve yönetmeliklere de tabi olmaktadır. (örn. Türk Ticaret Kanunu). Bu nedenle; bankacılık sektöründe faaliyet gösteren bankalar için tanımlanan riskler, diğer işletmeler içinde geçerli olmakla birlikte diğer işletmelere göre risklerin önem seviyesi değişkenlik gösterebilir. Bu değişkenlik seviyesi bankalardaki faaliyetlere temel oluşturan varlığın para olmasından dolayı ve fon arz ve talebi arasında aracılık görevi yerine getirildiğinden,

diğer sektörlere göre daha esnek olmayan bir yapıya sahip olmakla birlikte bazı risklerin seviyesi daha yüksek hissedilebilir.[114]

İşletme bünyesindeki riskler **Şekil 9** içerisinde belirtilmiş olup, bu riskler bankalar içinde geçerli olup, önem dereceleri değişiklik gösterebilmektedir. Bu riskler içerisinde yer alan risklerden bankalar için en önemli olan risk tanımı "Finansal Riskler"dir. Bankalar için sorun teşkil edecek ve diğer risk sınıflamalarından önce daha fazla etkileyecek olan risk grubu finansal risklerdir. Etki derecesi yüksek olan finansal riskleri iki ana grup içerisinde tanımlamak mümkündür. Bu riskler aşağıdaki belirtilen risklerden oluşur[115]:

1. Grup Sistematik Riskler: Sistematik riskler banka dışında gelişen değişikliklerden ve gelişmelere bağlı olarak ortaya çıkan riskleri oluşturur. (Faiz, Kur, Menkul Kıymet Fiyatları Riski)

2. Grup Değişken Riskler: Değişken riskler bankanın içerisinde bulunduğu piyasa koşullarından çok bankanın bilançosundan kaynaklanan ve borç-alacak portföyünün yapısına bağlı olarak ortaya çıkan risklerden oluşur. (Kredi, Likidite, Operasyon Riski)

Bankaların gerçekleştirmiş olduğu işlem ve faaliyetler dikkate alındığında, bankalar sürekli olarak riskli faaliyetler içerisinde yer almaktadır. Riskli faaliyetler içerisinde işlem yapılırken ortaya çıkan risklerden bazılarından kaçınabilmekte; bazılarından ise kaçınamadığı görülmektedir. Bankaların gerçekleştirdiği faaliyetler değerlendirildiğinde kaçınabildikleri risk grupları 3 ana grupta toplanabilir:[116]

---

[114] SAYIM ve ER, a.g.m., ss.12.

[115] SAYIM ve ER, a.g.m., ss.12.

[116] Pınar Evrim MANDACI, "Türk Bankacılık Sektörünün Taşıdığı Riskler ve Finansal Krizi Aşmada Kullanılan Risk Ölçüm Teknikleri", **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt 5, Sayı 1, 2003, s.69.

1) Karmaşık olmayan faaliyetler ile ayrıştırılabilen veya kaçınılabilen riskler: Bu grup içerisinde yoğunluklu olarak kullanılan risk kaçınma işlemleri 3 grup içerisinde sınıflandırılabilir,

a.1 İşletme üst yönetimi tarafından verilen kararların etkin ve verimli olması açısından süreç, sözleşme ve prosedürlerinin standart hale getirilmesi,

b.1 İşletmeye borçlu olan taraflar sınıflandırılarak ve/veya çeşitlendirilerek, verilen borç miktarına bağlı oluşabilecek olan kayıpların etkilerini azalmak amacıyla borçlu olan taraflara ait kredi portföyünün oluşturulması,

c.1 İşletme yönetimiyle yapılan, çalışanların sorumluluğunu içeren, çalışanları teşvike yönlendiren sözleşmelerin uygulanması,

2) Karşı tarafa transfer edilebilen riskler: Bu risk sınıf içerisinde yer alan riskleri transfer edebilecek, azaltabilecek ve/veya ortadan kaldırabilecek olan kontrol ortamları ve/veya işlemler bulunmaktadır.

3) Banka bünyesinde dinamik ve güncel olarak yönetilebilen riskler: Bu grup içerisinde sınıflandırılan risk çeşitleri, banka bünyesinde ortadan kaldırılabilecek veya kabul edilmesi gereken risk durumunu içeren iki farklı durum oluşabilir. Bu durumda banka düzeyindeki risk yönetiminde banka kaynaklarının kullanılması için nedenler oluşabilir. Bu durumlardan birisi, risk taşıyan varlık ya da faaliyetler karışık olmakla birlikte, bu durumun üçüncü taraflara transfer edilmesi güç ve/veya imkânsız olabilir. Belirtilen bu durum bankaların sahip olduğu varlıkların çok zayıf bir ikincil piyasalarının bulunmasından ve/veya hiçbir piyasasının bulunmamasından kaynaklanmaktadır. Banka tarafından karşılaşılan ikinci durum, bankanın risk ve beklenen getirileri nedeniyle kabul etmiş olduğu durumlarda ortaya çıkabilir. Bu kapsamda; bankanın operasyonları ile ilgili olarak amaçladığı işlemlerin ortasında bulunan riskler ortadan kaldırılabilir. Bu duruma örnek olarak banka bünyesinde kullandırılan kredilere ait kredi riski; bankanın sahip olduğu faaliyetler içerisinde yer alan piyasa riskini ifade eder.

2.2 Bankaların Sektör Bünyesinde Karşılaştıkları Temel Risk Çeşitleri

Bu çerçevede bankaların karşılaştıkları temel riskler dört kategoriye sınıflanabilir. Temel dört kategoriye ayrılan risk sınıfları sırasıyla; piyasa riski, kredi riski, likidite riski ve operasyonel risk şeklindedir.

Kredi Riski

Bankanın müşterileri ile yapmış olduğu sözleşme içeriklerine, standartlarına ve/veya gereksinimlerine müşteri tarafından uyulmaması buna bağlı olarak müşteri yükümlülüğünü kısmen veya tamamen zamanında yerine getirememesinden dolayı oluşan risk durumunu ifade eder.[117] Kredi riski; müşterinin yapmış olduğu sözleşmeye istinaden almış olduğu kredi bedelini ödememesi veya geç ödemesinden dolayı bankaya ait net kar ve özvarlığın içinde bulunduğu piyasa içerisinde ortaya çıkan değişimi ifade eder.[118] Kredi işlemleri içerisinde yer alan kredi sağlama fonksiyonu bankaların temel faaliyetini oluşturur. Kredi kullandırma işleminden önce müşterilerin kredibilitesi hakkında tam, doğru ve zamanında karar vermeye çalışır. Karar verme aşamasında yaşanan bazı durumlar, karar verme işlemini olumsuz yönde etkileyebilir. Bunun yanında doğru alınmış olan bir karar, kredi kullanacak olan tarafların zaman içerisinde kredibilitesinin azalmasına bağlı olarak değişkenlik gösterebilir. Bu durumda, bankalar teminat kalitesine bağlı olarak, kredi riski ile karşılaşma olasılıkları artabilir. Bankalar sadece kredi operasyonlarına bağlı olarak kredi riski taşımamaktadır. Bankacılık faaliyetlerinde, banka bilanço ve bilanço dışı hesaplarda yer alan işlemlerde bankalar kredi riski ile karşı karşıya gelirler.[119] Banka bünyesinde karşılaşılan kredi riskinin zamana bağlı olarak artış göstermesi, borcun ve öz kaynağın marjinal maliyetini arttırır. Bu nedenle banka içerisinde uygulanacak olan kredi risk yönetimi uygun parametreler

---

[117] BDDK, "Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmelik", 08.02.2001.

[118] MANDACI, a.g.m., ss.72.

[119] BDDK, "Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmeliğin Uygulanmasına ilişkin 1. Sayılı Tebliğ", 08.02.2001.

dahilinde bankanın karşılaşabileceği riskleri yönetmeyi iş planına dahil ederek, bankanın karşılaştığı risklere ait getirileri maksimum seviyeye çıkartmayı hedefler.[120]

Kredi riski, tahsis edilen kredi tutarına ait ödeme işlemlerinin tam, doğru ve zamanında yapılmamasına bağlı olarak bankaya ait net kâr ve özvarlığında ortaya çıkacak olan değişimi ifade eder. Kredi riski aşağıdaki belirtilen kriterlerden oluşur:[121]

• Banka bünyesinde tahakkuk edilmiş ancak tahsil edilememiş faiz değeri,

• Krediye ait oluşan borç miktarının belgelendirilmesi, yeniden yapılandırma analizi, borç miktarına ait sahip olan taraf bilgisinin değişikliği ve kredinin satış ve pazarlanmasına ait yönetim giderleri ve diğer giderler,

• Takipte olan kredilere ait yasal uygulamaya bağlı olarak oluşan takip giderleri,

• Kredi kullandırılan müşterinin krediye ait borçlarını tam, doğru ve zamanında ödememesine bağlı olarak tahsil edilecek olan borç tutarına ait faiz getirisinin sağlanamaması durumunda oluşan fırsat maliyeti,

Bankalar bünyesinde kredi riskinin içeriğini birkaç risk başlığı oluşturmaktadır. Bunlar;[122]

1) Esas Kredi Riski: Banka tarafından kredi tahsisi yapılan müşterinin sözleşme koşullarını yerine getirmemesine bağlı olarak esas kredi riski oluşur. Bu durumun oluşması, tahsis edilen kredi tutarına ait bir kaybın oluşmasına neden olabilir. Borç veren banka sözleşme koşulları nedeniyle ortaya çıkabilecek olan riski garanti altına alabilmek amacıyla borç sözleşmesine ait temin edilmesi gereken teminat, kefalet vb.

---

120 M. Barış AKÇAY ve K. Evren BOLGÜN, **Risk Yönetimi: Gelişmekte Olan Türk Finans Piyasasında Entegre Risk Ölçüm ve Yönetim Uygulamaları**, 2. Baskı, Scala Yayıncılık, İstanbul, 2005, s.201.

121 Osman ÖZÇELİK, "Bankacılıkta Risk Analizi, Yönetimi ve Riskten Korunma", **Yüksek Lisans Tezi,** Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Edirne, Ocak 2006, s.10.

122 ÖZÇELİK, a.g.e., s.12-13.

enstrümanların değerini arttırabilir. Bu enstrümanlar riskin oluşma olasılığının azalmasını sağlamak amacıyla kullanılır.

2) Yazılma Riski: Bankaların finansal işlemleri arasında finansal kıymetleri kullanmaktadır. Bankalar tarafından kullanılan finansal kıymetler ikincil piyasalarda alınır ve satılır. Finansal kıymetlerin ikincil piyasada işleme tabi olması sırasında alıcıya ait kredi koşulları ile uyuşmamasına istinaden oluşan risk çeşidi yazılma riski olarak tanımlanır.

3) Yerleşme Riski: Bu durum kredi sözleşmesine taraf olan sorumlulardan birinin sözleşmeyi yerine getirmemesinden kaynaklanabilir. Bu durum bankacılık sektöründe faaliyet gösteren kredi sağlayıcıların kredi tahsisi aşamasındaki kredi birim fiyat dalgalanmalarına bağlı olarak ortaya çıkabilir. Kredilerin işlem gördüğü piyasa içerisindeki fiyat dalgalanmaları arttıkça, sözleşmeye taraf olan müşterinin sözleşmeyi tamamlamaktan kaçınması olasılığı artmaktadır. Bu durum yerleşme riskinin artmasına neden olacaktır.

4) Belgelendirme Riski: Banka bünyesinde gerçekleştirilen kredi sözleşmesine ait dokümantasyon işleminin tam, doğru ve zamanında yapılmamasına bağlı olarak oluşan risk türünü ifade eder. Bu riskin azaltılmasının yöntemi; banka bünyesinde oluşturulan ve müşteriye verilen kredi sözleşmelerin standart bir format dahilinde oluşturulması ve format içerisinde yer alan bilgilerin tam ve doğru bir şekilde müşteri tarafından doldurulmasının sağlanmasıdır.

5) Olay Riski: Bankanın kredi müşterilerine ait mali yapılarının beklenmedik durumlar ve olaylar sonucunda değişmesi ve buna bağlı olarak verilen kredi için risk ortamının değişmesine bağlı olarak ortaya çıkan risk türüdür.

6) Operasyon Riski: Banka yönetimi içerisinde kredi riskine bağlı olarak ortaya çıkan sorunlarla ilgili olarak banka bünyesinde oluşan ve/veya oluşması beklenen zararlar ile karşılaşılması durumunda oluşan risk türünü ifade eder.

Piyasa Riski

Bankanın bilanço içi ve dışı hesaplarda izledikleri varlık ve pozisyonlarının bağlı oldukları cari piyasa değerlerinin düşmesine bağlı olarak bankanın karşılaşabileceği kayıp miktarına bağlı olarak ortaya çıkması beklenen kayıp olasılıklarını ifade eder. Genel kabul görmüş, uluslararası muhasebe standartlarına göre bankalardaki piyasa riskinin temelini oluşturan varlık ve pozisyonların cari piyasa fiyatları üzerinden değerlenmesini zorunlu kılar.[123]

Bankanın bünyesinde yer alan varlık yapısının piyasadaki değeri ve bu piyasa değerine bağlı olarak gelecekteki beklentileri etkileyen makro gelişmeleri piyasa riski açıklar. Makro gelişmelerle birlikte piyasa içerisinde ortaya çıkan dalgalanmalara bağlı olarak faiz, kur ve hisse senedi fiyatlarının değişmesine neden olabilir. Bu durum bankanın bilanço ve bilanço dışı işlemlerinde zarar etmesine veya beklenenden daha az miktarda kâr elde etmesine neden olur. Piyasa riski bir sistematik risk olarak tanımlanmakla birlikte; bu tür bir riske engel olmak mümkün olmayabilir. Piyasa riski herhangi bir zaman dilimi içerisinde oluşabilir. Bu bakımdan piyasa riski değerlendirildiğinde piyasa riskini transfer edip, etkisini azaltacak süreç ve yapılar işletme bünyesinde oluşturulmaya ve geliştirilmeye çalışılır.

Kur Riski

Bankaların bünyesinde oluşturdukları pozisyon içerisinde yer alan yerli paranın, yabancı paralar karşısında değer artışı ya da değer kaybı oluşması halinde oluşan risk türü kur riski olarak tanımlanmaktadır.[124] Kur riski, bankaların nakit akımlarında, gelir ve giderlerinde kur değişimine bağlı olarak ortaya çıkabilecek olan dalgalanmaların ve değişimlerin oluşma ihtimalini ifade eder. Yani bankaların yabancı para cinsinden olan yükümlüklerinin, yabancı para cinsinden olan varlıklarına eşit olmaması durumunda kur riski oluşur. Bankaların almış olduğu döviz pozisyonlarının yanında aldıkları döviz

---

[123] Kemal Çağatay ŞİMŞEK, "Bankacılıkta Risk ve Risk Ölçüm Yöntemleri", **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2007, s.10.

[124] Ziya Tunç ALOĞLU, "Bankacılık Sektörünün Karşılaştığı Riskler ve Bankacılık Krizleri Üzerindeki Etkileri", **Uzmanlık Yeterlilik Tezi**, TCMB Bankacılık ve Finansal Kuruluşlar Genel Müdürlüğü, Mart 2005, s.37.

pozisyonlarına ait değişikliklerde önemlidir. Bankaların net döviz pozisyonları üç farklı şekilde oluşur. Bunlar açık, kapalı ve kare pozisyon olarak oluşmaktadır.

Net Döviz Pozisyonları	
Short (Açık Pozisyon)	Döviz Yükümlülükler > Döviz Varlıklar
Long Position (Kapalı Pozisyon)	Döviz Varlıklar > Döviz Yükümlülükler
Square (Kare Pozisyon)	Döviz Varlıklar = Döviz Yükümlülükler

Şekil 11: Bankalarda Net Döviz Pozisyonları

Açık pozisyon tanımına örnek olarak; yabancı paranın değer kaybına uğrayacağı veya yerli paraya ait alternatif getirinin daha yüksek olacağı düşünülerek, bankaların ucuz yabancı para birimleriyle borçlanıp, bu kaynakları yerel paraya çevirerek kâr elde etme amacıyla tuttuğu pozisyonlar olarak tanımlanabilir. Kapalı pozisyon açık pozisyonun tam tersi beklentilerin olduğu durumu ifade eder. Kare pozisyon ise bankanın döviz varlık ve yükümlülüklerinin tam olarak eşit olduğu durumdur. Bu durumda dövizin değer değişiklikleri bankaları olumlu veya olumsuz olarak etkilememektedir.

Bankaların mali yapısının ve rekabet güçlerini etkileyen ve değişmesine neden olan faktörler; bankanın döviz cinsinden varlıkların ve yükümlülüklerin ulusal para değerine dönüştürüldüğü ve varlıkların fiili olarak satılacağı veya banka yükümlülüklerin geri ödeneceği zaman, kurlarda meydana gelen değişiklik ve belirsizliklerdir. Döviz kuru riskine açık olan bankaların bu riskten şiddetli bir şekilde etkilenmesi likidite krizinin oluşmasına neden olabilir. Türkiye'de yaşanan 2001 krizinden önce kurlarda meydana gelen artışlar, tüm bankaların açık pozisyonlarını eş zamanlı kapatmalarına neden olmakla birlikte kurların artmasına hem de ulusal para cinsinden varlıkların satışında likiditenin azalmasına ve faiz oranlarının beklenmedik miktarlara çıkmasına neden olmuştur. Bu durumun oluşması alım satımda kur ve faiz artışının oluşmasıyla birlikte; zarara uğrayan bankaların döviz cinsinden yükümlülüklerinin artmasına neden olmuştur.

Yükümlülüklerin artması bankalara ait maliyet yapılarının değişmesine bağlı olarak gelecekteki karlılıkların azalmasına neden olmuştur. Bunun yanında kurda yaşanan artış döviz cinsinden kredi kullanan müşterilerin kredi miktarlarını bankaya geri ödemelerinde sorun yaşamalarına neden olmuştur. Kur riskinin bankalara ve banka müşterilerine olan etkisi değerlendirildiğinde; bankaların kur riskine bağlı olarak karşılaşılan zararın boyutu daha iyi anlaşılabilir.

Faiz Riski

Bankanın finansal pozisyonunun ve durumunun faiz oranında meydana gelen değişikliklere istinaden olumsuz yönde etkilenmesi olasılığı faiz riski olarak tanımlanmaktadır. Faiz faktörü banka gelirleri ile bilanço içi ve bilanço dışı kalemlerinin ekonomik değerleri üzerinde önemli bir etki alanı bulunmaktadır.

Faiz riski banka bilanço kalemleri içerisinde aktif-pasif arasında faize duyarlı kalemlerin miktarında veya söz konusu kalemlere ait vade, faiz çeşitlerinde ve oranlarında bir uyumsuzluk olduğu durumlarda oluşur. Banka içerisinde ortaya çıkan uyumsuzluklar net faiz geliri marjı değişimi olasılığının artmasına neden olarak bankaya ait kârlılığın etkilenmesine neden olur. Banka bünyesinde faize duyarlı pasif toplamı faize duyarlı aktif toplamından yüksek ise faiz oranı içerisinde meydana gelen değişiklikler kâr miktarının azalmasına neden olur.[125] Faiz gelirine ait marj miktarı, faize duyarlı aktiflerin pasiflere göre daha uzun vadeli olması durumda daralır. Faiz faktöründe meydana gelen değişiklikler, banka bünyesindeki faize duyarlı aktif ve pasif miktarına ait vade yapılarının uyumlu olması durumunda net faiz marjı üzerinde herhangi bir etkisi olmamaktadır. Bunun yanında değişken faizli olan mali yükümlülük miktarı varlık miktarından yüksek ise bu durum bankanın gelecekte elde edeceği nakit akımlarında belirsizliklerin ve dengesizliklerin oluşmasına neden olabilir. Faiz riski aşağıdaki belirtilen koşulların oluşması durumunda ortaya çıkabilir:

[125] Suat Teker, "Aktif-Pasif Yönetimi", T.B.B Eğitim Notları, İstanbul, 14-16 Şubat 2001, s.20.

1) Yeniden Fiyatlandırma Riski; faiz oranlarının değişmesine bağlı olarak aktif ve pasif içerisinde faize duyarlı olan kalemlerin fiyatlarının yeniden hesaplanmasına bağlı olarak faiz gelirinin değişmesine yönelik olarak oluşan risk türünü ifade eder.

2) Gelir Eğrisi Riski; banka gelir eğrisinde meydana gelen değişimlerin bankanın net faiz gelirini ve ekonomik değerini olumsuz etkilemesi riskidir. Banka ürünlerine ait fiyatlandırma işlemlerindeki farklılıklar, bankaya ait olan getiri eğrisinde oluşan eğim açısının ve şekil yapısının değişmesine neden olmaktadır.

3) Baz Riski (Basis Risk); aynı fiyatlandırma özelliklerine sahip farklı finansal araçlara ait faiz oranlarının kalibrasyonlarında yapılan hatalı korelasyondan kaynaklanır.

Bankalarda faiz faktörüne ait faiz risklerinin iyi yönetilmesi durumunda bu durum bankalar için önemli bir kâr kaynağı oluşturmaktadır. Faiz oranlarındaki değişimin analiz edilmesi ve tahmin edilerek banka pozisyonun revize edilmesi durumunda bankaya ait karlılık oranı ve miktarında artış gözlenebilir.[126] Türkiye'de faaliyet gösteren bankaların genel olarak pasifleri değişken faizli ve kısa vadeli mevduatlar ile kısa vadeli yabancı kaynaklardan oluşurken, aktiflerinde ağırlıklı olarak sabit faizli ve uzun vadeli yatırım araçları ile yine sabit faizli kredilerden oluşmaktadır. Faiz oranlarında meydana gelecek olan değişiklikler ve yükselmeler tüm bankaların net faiz marjının hareket kabiliyetini azaltmakta ve kârların azalmasına ve uzun vadeli finansal araçların satışında piyasa koşullarının tam ve etkili bir şekilde oluşmamasına bağlı olarak, talep yetersizliği kapsamında satış zararlarının ve likidite sorunlarının oluşmasına neden olabilir.

Likidite Riski

Likidite riski, bankaların fon ihtiyaçlarını tam, doğru ve zamanında karşılayamaması ve/veya zorluk yaşaması durumunda karşılaştığı risk türünü ifade eder.[127]

---

126 BDDK, " Bankacılık Değerlendirme Raporu", Ekim 2004, s.56.

127 ALOĞLU, a.g.e., s.22-23.

Bu risk banka bilanço pasif kalemlerindeki artış miktarını ve aktif kalemlerindeki artış miktarını iyi yönetememesi durumda oluşmaktadır. Olağan dışı durumlardaki likidite yetersizliği bankaların yükümlülüklerini yerine getirememesine neden olabilir.[128]

İşletmelerde karşılaşılan likidite riski, işletmelerin katlanabileceği standart maliyetlerle kaynak oluşturabilme gücü ve ihtiyaç duyulan likidite sınırı olarak tanımlanabilir. İhtiyaç duyulan likidite seviyesinin üzerine çıkılması, işletmeye ait kısa vadeli olan yükümlülüklerini veya nakit çıkış miktarlarını karşılama kabiliyetini kaybetmesi durumunda likidite riski oluşabilir.

Bankalar yapmış olduğu işlemler ve banka finansal yapısı gereği üstlenebilecekleri düzeyde masraf ve maliyetlerle işletmeye kaynak sağlayabilir. Bu durum, kaynak sağlayabilme gücüne bağlı olarak değişkenlik gösterebilir. Bankaların kaynak sağlayabilme gücü sadece bankaların elinde olmayıp, bu güç piyasanın ve bankanın likiditesine göre değişkenlik göstermekle birlikte; banka için fonlama niteliklerinin belirlenmesinde görev alır.[129] Bankalar, özellikle bünyelerinde bulunan mevduat ürünlerine ait müşterilerden gelecek olan çekme işlemlerinde oluşabilecek olan belirsizlik nedeniyle likidite problemi yaşamamak için getiri oranı düşük ve/veya hiç olmayan fon kaynak yatırımlarına bünyelerinde yer verir. Bünyelerinde yer verdikleri fon kaynak yatırımlarına banka yönetimi karar verir. Banka yönetimi karar aşamasında gelir, likidite ve risk faktörleriyle karşılaşır. Bu karşılaşılan kavramların yönetilmesi işlemine likidite risk yönetimi adı verilir.[130]

Türkiye'deki bankalarda yaşanan likidite riski genelde varlık ve yükümlülüklerin vadelerinin farklı ve/veya uyumlu olmamasına bağlı olarak ülke koşulları ve risk ortamına bağlı olarak oluşmaktadır. Bunun yanında sahip olunan banka

---

[128] Selahattin KOÇ, "Bankaların Karşılaştıkları Riskleri Yönetmedeki Etkinliği: Türkiye Ölçeği", **Maliye Dergisi**, Sayı:165, Temmuz-Aralık 2013, s.279.

[129] D.G. UYEMURA, **Financial Risk Management in Banking**, Bankers Publishing Company, Chicago, 1993, s.234 – 235.

[130] Gökhan BİLGE, "Bankalar Açısından Risk Yönetiminin Önemi ve Basel II Sürecinin Risk Yönetimi Üzerindeki Etkileri", **Yüksek Lisans Tezi**, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta, 2011, s.7.

varlıklarının nakde dönüştürülmesinde piyasaların geniş ve gelişmiş bir piyasa olmaması likidite riskini arttırmaktadır. Banka bünyesindeki aktif ve pasif kalemlere ait faize duyarlılıkların uyuşmaması, faiz hareketlerinde oluşacak olan volatililerde banka bünyesinde bir likidite sıkıntısı yaşanmasına neden olabilir. Bunun yanında banka portföyü içerisinde döviz cinsinden olan varlık ve yükümlülükler, döviz kurundaki değişikliklere göre bankaların likidite riskinin ve açık pozisyonun oluşmasına neden olabilmektedir. Bu açıdan bakıldığında; faiz ve döviz kurlarının likidite riski üzerindeki etkisi yüksek olmakla birlikte bu durumun likidite risk hesaplamasında dikkate alınması sağlanmalıdır. Bankacılık sektöründe faaliyet gösteren bankaların faiz ve likidite riski almayı tercih etmeleri bankacılık faaliyetini yürüttüklerini göstermektedir.

Operasyonel Risk

İşletme içerisinde yer alan verimli ve etkili olmayan operasyonlara ait süreçlerden, personel veya dış faktörlere ait olaylara bağlı olarak oluşan risk çeşitleri operasyonel risk olarak tanımlanır.[131] Bankacılık sektöründe ise; banka bünyesindeki iç kontrol faaliyetlerinde ortaya çıkan hatalar ve/veya eksiklikler nedeniyle operasyonel faaliyetlerdeki hata ve usulsüzlüklerin tespit edilememesi, banka bünyesinde görev alan üst yönetim ve çalışan insan kaynağının değişen zaman ve koşullara uyumlu olarak aksiyon alamaması, banka operasyonlarında yer alan bilgi sistemlerindeki hata ve duraksamalara bağlı olarak yaşanabilecek olan kaynak kayıpları ve/veya zarara maruz kalma ihtimali olarakta tanımlanabilir.[132] Operasyonel risk, kredi ve piyasa risk türlerine göre daha kapsamlı bir türü olmakla birlikte; proses açıklamaları ve tanımlamaları diğer risk türlerine göre daha açık ve net yapılabilir. Operasyonel risk türü özelinde veri tabanı oluşturulması ve bu veri tabanını besleyecek olan entegre bilgi sistemlerinin tanımlanması, söz konusu risk türünün kapsamını ve çalışma alanını genişletmektedir.[133] Teknolojinin ve kullanılan ürün çeşidinin ve sayısının hızla gelişmesi, iş akışlarının karmaşık bir hale gelmesi ve sistem içerisinde yer alan kontrol işlemlerinin güçleşmesine

---

[131] Basel COMMITTEE, "Operational Risk", 2001, http://www.bis.org/publ/bcbsca07.pdf, (15.10.2005), s.10.

[132] BDDK, "Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmelik", 08.02.2001.

[133] AKÇAY ve BOLGÜN, a.g.e., s.204.

bağlı olarak, hata ve hileye dayalı olan operasyonel risklerin artmasına neden olmuştur. Bu gelişmeler değerlendirildiğinde; Basel Komitesi, Basel II kriterinde sermaye yeterliliği hesaplamasını gerçekleştirirken operasyonel risk türünü de dikkate almıştır.

2.3 Bankaların Karşılaştığı Diğer Risk Türleri

Bankacılık sektöründe faaliyet gösteren bankaların gerçekleştirdiği faaliyetler dikkate alındığında risk evrenlerinin çok fazla geniş olduğu görülür. Bu nedenle bankacılık sektöründe yukarıdaki tanımlanan riskler dışında birçok risk türü ile karşılaşılmaktadır. Karşılaşılan riskler arasında itibar riski ve yasal risk önemli bir yer tutar.

Faaliyet gösterilen sektör içerisindeki kamuoyuna ait olumlu olmayan görüşlerin bankalara ait faaliyet ve gelirleri üzerindeki mevcut ve olası etkileri itibar riskini ifade eder. Bankacılık işlemlerinde müşterinin kabulünden müşterinin verilerinin korunmasına kadar birçok örnek kapsamında bankalar, güven esasına dayalı olarak faaliyet gösterir. Dürüstlük ve güven kavramı bankaların sahip olduğu en önemli ve görünmeyen değerli aktif kalemlerinden biridir. Bankanın mevcut durumda edindiği ve edinmeyi planladığı müşterilerin güvenlerini kazanması ve bu güveni hiç taviz vermeden muhafaza etmesi önemlidir. İtibar riski bankalar için önemli bir risk türü olmakla birlikte söz konusu bu risk türüne maruz kalınılması banka bünyesinde önemli hasarların oluşmasına neden olabilir.[134]

Bankanın uymakla yükümlü ve sorumlu olduğu kural, kanun ve/veya yönetmelik kapsamında banka tarafından ihlallerin oluşması ve/veya uyulmaması durumunda ortaya çıkan ve/veya çıkabilecek olan kayıp ihtimalleri yasal risk olarak tanımlanmaktadır.[135]

Bankacılık ve diğer işletmelerde karşı karşıya kalınan diğer risk türü ise, **doğal risktir.** Banka ve/veya işletme bünyesinde gerçekleştirilen muhasebe işlemlerinde uygulanması gereken iç kontrol işlemleri dikkate alınmadan yapılması durumunda ortaya çıkabilecek olan hatalar ve/veya yanlışlıkların oluşma olasılığı doğal risk olarak

---

[134] İnönü Akgün ALP, "Bankalarda Karapara Aklama Risk Yönetimi", **Active Bankacılık ve Finans Dergisi**, Sayı:145, Ocak-Şubat 2005, s.4.

[135] BİLGE, a.g.e., s.10.

tanımlanır. Doğal risk tanımına bağlı olarak kontrol faaliyetleri ile ilgili olarak **kontrol riskleri** oluşabilir. Doğal risk miktarını ve etkisini azaltabilmek amacıyla banka bünyesinde iç kontrol sistemleri oluşturulur. İç kontrol sistemleri oluşturulurken, risklere yönelik olarak kontrol faaliyetleri uygulanır. Kontrol riski iç kontrol sistemi içerisinde oluşan önemli bir hatayı ve/veya yanlışlığın zamanında, tam ve doğru bir şekilde ortaya çıkartılamaması olasılığını ifade eder. Kontrollerin etkili bir şekilde tanımlanması, çeşitli sınırlandırmalar nedeniyle belirli seviyede kontrol riskinin oluşma ihtimalini engellememekle birlikte, kontrol riski oluşma ihtimalini minimum seviyeye indirgemektedir.[136]

2.4 Bankalarda Bilgi Sistemleri Riskleri

Bilişim sektörünün gelişmesi ile birlikte bankacılık sektöründe kullanım miktarı ve sıklığı artış göstermiştir. Bankacılık sektöründe bilişim sektörünün yoğunluklu olarak temel iki alanda kullanılmaya başlanmıştır.[137]

1) Banka İçi Otomasyon: Banka içi otomasyon işlemleri ön ve arka büro bankacılık işlemleri olarak tanımlanabilir. Müşterilerin para çekme, para yatırma, çek senet işlemleri ön büro bankacılığını oluştururken, yılsonu işlemleri, bankanın muhasebe işlemleri ve iç haberleşme sistemi arka büro bankacılığını oluşturmaktadır.

2) Banka Otomasyonu: Müşteriye yönelik olarak yeni hizmetlerin ve tekniklerin oluşturulması banka otomasyonun temel amacını oluşturmaktadır. Bu kapsamda bankalar bünyesinde kullanılan tekniklere örnek olarak ise aşağıdaki uygulamalar verilebilir.

- POS, Banka Kartları, Kredi kartları,
- Otomatik vezne makineleri (ATM),
- Internet Bankacılığı

[136] BOZKURT, İBİŞ ve AKDEMİR, a.g.m., ss.170-171.

[137] BAŞARIR, a.g.e, s.37.

- Telefon Bankacılığı
- Televizyon Bankacılığı vb.

Mevcut yapı içerisinde teknolojinin önemi ve hızı artış göstermektedir. Bankalar sahip oldukları varlıklara ait kayıpları yaşamamak amacıyla; teknolojik yenilikleri organizasyon yapısına dahil ederek, hizmetlerini bu doğrultuda sunmaktadır. Bankaların, organizasyon yapısı içerisinde yeni teknolojileri kullanmasının nedeni aşağıdaki belirtilen faktörler ile açıklanabilir:[138]

1) Maliyet unsuru,
2) Bankalar arası rekabet,
3) Bilgi toplumunun talepleri,
4) Yeni hizmet ve ürün anlayışı,
5) Bilgisayar teknolojisindeki gelişmeler,
6) Yeni sistemin sağladığı verimlilik vb.

Yukarıdaki belirtilen bilgilerden hareket ile teknolojinin bankacılık sektörü içerisinde önemli bir yerde bulunduğu düşünüldüğünde; bankacılık sektöründeki bilgi sistemleri riski önem arz etmektedir. İş süreçlerine ve faaliyetlerine olumsuz olarak etki edecek bir şekilde bilgi sistemi uygulamalarının, ağ veya diğer kritik bilgi teknolojileri kaynaklarının kaybedilmesi olasılığı bilgi sistemleri riski olarak tanımlanmaktadır.

Bilgi teknolojileri riskleri genel olarak faaliyet bazında oluşturulan organizasyona ait iş risklerinin içerisinde bulunmakta ve diğer risk tanımlamaları ile bütün olarak değerlendirilmektedir. Örneğin, banka bünyesinde değişen sektör koşullarına istinaden yapılması zorunlu öngörülen bilgi sistemleri altyapısındaki değişiklikler, sistemin beklenmedik tepkiler vermesine bağlı olarak geri getirilemeyecek bir şekilde problemlerin yaşanmasına ve/veya hasara uğramasına neden olabilir. Bu

[138] BAŞARIR, a.g.e., s.38.

durum, bankanın faaliyetlerinin aksamasına bağlı olarak gelir kaybı riskinin oluşması ile sonuçlanabilir. Günümüzde bankacılık sektöründe faaliyet gösteren bankaların, veri ve bilgi teknolojileri altyapılarına olan bağımlılıkları yüksektir. Bilgi teknolojileri riskleri iş riskleri ve yönetim stratejileri ile birlikte bir bütün olarak değerlendirilir. Bu nedenle bilgi teknolojileri riskleri banka içerisindeki karşılaşılan tüm risklerle birlikte tanımlanmalı, değerlendirilmeli, ölçülmeli ve yönetilmelidir.

2.5 Bilgi Teknolojileri Risk Tanımı ve Operasyonel Risk İle Bağlantısı

Bu bölüm içerisinde bankacılık sektörü içerisinde yoğun olarak kullanılan bilgi teknolojileri uygulamalarına ait risk tanımına yer verilecek olup, tanımı yapılan bilgi teknolojileri risklerinin operasyonel riskler ile olan ilişkisi anlatılmaya çalışılmıştır.

Basel komitesi yaklaşım olarak operasyonel riskin, işletme bünyesinde gerçekleştirilen süreçlerden, süreç içerisinde görevli olan çalışanlardan ve işletme dışında gerçekleşen olaylardan oluştuğunu ve nedenlere dayandığını kabul eder.[139] Benimsenen bu yaklaşım içerisinde, bankalar bünyesinde yürütülen faaliyetlere ait risklerin süreç içerisinde kullanılan bilgi sistemleri risklerine bağlı olarak oluştuğu vurgulanmıştır.

2.5.1 Bilgi Teknolojileri Risk Tanımı

İşletme yönetiminde görev alan yöneticiler işletmeye yön verebilmek amacıyla karar alırlar. İşletme yöneticileri karar verebilmek için bilgi ve verilerden yararlanır. Bilgi sistemlerinin amacı; yöneticilerin ihtiyacı olan bilgi ve veriyi tam, doğru, zamanında ve hızlı bir şekilde temin ederek; ilgili yöneticilerin ihtiyaç duyduğu format dahilinde işlenmesini ve düzenlenmesini sağlamaktır.[140]

Bilgi, yöneticilerin karar almasına yardımcı olur. Verilerin işlenmiş hali, bilgi olarak ifade edilir. Verilerin işlenmesi; toplanması özetlenmesi ve karar alınacak ve istenilen format haline getirilmesi olarak tanımlanabilir. Veri kavramı bilgiye ulaşmada

---

[139] Murat MAZIBAŞ, **"Operasyonel Riske Basel Yaklaşımı: Risk Verilerine İlişkin Bir Değerlendirme"**, BDDK Araştırma Raporları, Temmuz 2005, s.3.

[140] Faruk ÇUBUKÇU, "İşletme Yönetimi ve Bilgi Sistemleri", Yüksek Lisans Tezi, http://www.farukcubukcu.com/images/docs/yonetimbilgisistemleri.htm, (19.06.2007), s.1-2.

kullanılan bir araç olarak nitelendirilebilir. Doğru bilgiye zamanında ulaşabilmek adına gerçekleştirilen bilgi işleme süreci, ayrı bir faaliyet olarak nitelendirilebilir.[141]

İşletme yönetimde tüm çalışanlar bilgiyi kullanır. Bilgiyi kullanma ve ihtiyaç düzeyi yönetim kademesine göre farklılık gösterebilir. İşletme içerisinde üretilen ve/veya dış kaynak aracılığıyla temin edilen bilgiler; üst yönetim tarafından planlama ve kontrol gibi yönetimsel fonksiyonlar için gerekli olup, organizasyon şeması içerisindeki diğer çalışanlar için operasyonel ve günlük işlemlerin etkili bir şekilde yürütülmesi açısından gerek duyulur.[142]

	Ana Konular	**Kaynak**	**Zaman Aralığı**	**Tipi**
Üst-Yönetim	Stratejik	Dış	Uzun	Yapısal değil
Orta-Düzey	Taktik	Dış/İç	Orta	Yarı Yapısal
Birinci Kademe Yönetim	Yapılan İşle İlgili	İç	Kısa	Yapısal

Şekil 12: Yönetim Düzeyine Göre Gereksinim Duyulan Bilgi
Kaynak: Reymond MCLEOD, **Management Information Systems**, 4.b., New York: Macmillan, 1990, s.19.

Yukarıdaki şema içerisinde belirtildiği gibi; bilginin farklı kaynaklardan ve farklı zamanlarda temin edilmesi buna bağlı olarak gereksinim duyan tarafların farklılaşması, bilgi sistemlerinin oluşturulmasına neden olmuştur. Bilgi teknolojileri işletmeler için operasyonel gelişme ve büyüme için fırsat ve yarar sağlamakla birlikte; beraberinde birçok tehlike (kesintiye uğrama, hileli işlemler, bilgilerin çalınması vb.) getirmektedir. Yapılan araştırma ve çalışmalar; bilgi teknolojilerinde kullanılan sistemlere işletme dışından yapılan saldırı, tehdit ve/veya müdahalelerin, işletme içerisinden yapılacak olan tehditlerden daha az olduğunu göstermiştir. Bu durum nedeniyle iş süreçlerinde bilgi teknolojilerinin rolünün artması beraberinde bilgi

[141] Özgür SELVİ, "Bilgi Toplmu, Bilgi Yönetimi ve Halkla İlişkiler", **Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi**, Sayı:3, Mart:2012, s.202-205.

[142] ÇUBUKÇU, a.g.e., s.1-2.

teknolojileri risklerinin analiz edilmesinin önemini arttırmıştır. Önemin artması beraberinde aşağıdaki yer alan soruların cevaplarının aranmasına neden olmuştur:[143]

1) İşletme bünyesinde korunacak olan nedir? Bütün işletmeler için "Güven" kavramının korunması gereklidir çünkü "güven" kavramı iş ve etkinliği sağlar. "Güven" kavramı bankacılık sektörünün temelini oluşturan bir faktör olduğu için bankaların faaliyetleri içerisindeki kontrol faaliyetlerini oluştururken "güven" faktörünü en öne alarak ilgili kontrol yapılarını oluşturmaları sağlanır. Kontrol kavramı, güven kavramını en temel seviyede korumaktadır. Bilgi teknolojileri ve bilgi sistemleri birçok operasyonel kontrollerin temelini oluşturmaktadır.

2) Bilgi teknolojileri kontrolleri hangi alanlarda uygulanır? İşletmenin yapısı ve gereksinim duyulan bilgilerin önemi kapsamında işletme bünyesinde bilgi teknolojileri kontrolleri her faaliyette ve her alanda kullanılabilir. Bilgi teknolojileri, iş süreçlerini, işletme bünyesindeki çalışanları ve işletme organizasyonunu içerir. Bankacılık sektöründe yürütülen işlemler değerlendirildiğinde, birçok işlem ve faaliyet içerisinde bilgi teknolojileri alt yapısı ve kontrolleri kullanılmaktadır. Banka bünyesinde yürütülen işlemler kapsamında bilgi teknolojileri kontrollerinin etkin ve verimli bir şekilde kullanılması, müşterinin bankaya olan güven katsayısının artmasını sağlamaktadır.

3) Bilgi teknolojileri kontrollerinden kim sorumludur? Bilgi teknolojileri kontrollerinden işletme bünyesinde yer alan bütün organizasyon yapısındaki görevli olan personel sorumlu olmakla birlikte; kontrol ile ilgili sorumluluklar işletme bünyesindeki üst yönetim tarafından belirlenmektedir. Bilgi teknolojileri kontrollerinden banka bünyesinde hangi bölüm ve/veya sorumlu kişilerin sorumlu olacağı regülasyonlar kapsamında değerlendirilmiş ve belirtilmiştir. (örn. Basel uygulamaları, BDDK tarafından oluşturulan yönetmelik ve/veya kanunlar kapsamında)

---

[143] Steve MAR, Rune JOHANNESSEN, Stephen COATES, Karine WEGRZYNOWİCZ ve Thomas ANDREESEN, **GTAG (Global Technology Audit Guide)-Information Technology Risk and Controls**, 2 Edition, March 2012, s.3.

4) Bilgi teknolojileri riskleri ve kontrolleri ne zaman değerlendirilmelidir? Bilgi teknoloji riskleri ve kontrolleri dinamik olarak her zaman değerlendirilmekle birlikte; işletme organizasyon yapısının ve süreçlerde ortaya çıkan değişikliklere göre değişkenlik gösterebilir.

5) Bilgi teknolojileri risklerine ait ne kadar kontrol yeterlidir? Bu sorunun cevabı; işletme bünyesinde görev alan üst yönetimin risk iştahına, toleransına ve zorunlu yasal uygulamalara bağlı olarak değişmektedir. Kontroller bir hedef değil, kontroller iş hedeflerine ulaşmaya yardımcı olan bir araçtır.

İşletme bünyesinde yürütülen işlemlere ait faaliyetleri olumsuz yönde etkilemesi muhtemel otomasyon ve/veya ağ sistemine bağlı olan kaynakların kaybolma ihtimali bilgi teknolojileri riski olarak tanımlanır.[144] Bilgi teknolojileri riski; gerçekleştirilen operasyonel işlemlere ait oluşan operasyonel riskler içerisinde payı artan bir risk olarak ortaya çıkar. Bu durum, işletmeler tarafından, bilgi sistemleri süreçlerinin ve bilgileri saklamayı otomatikleştirme işlemine bağlı olarak, bilgi sistemleri risk yönetimini ayrı bir uygulama alanı olarak kullanmaya başlamalarına neden olmuştur. İşletmelerin bu durumdaki faaliyetleri; organizasyon bütünü içerisinde faaliyet gösteren fonksiyonlarını, geniş kapsamlı risk odaklı bir bilgi sistemleri yaklaşımı ile konsolide etmişlerdir.[145]

2.5.2 Bilgi Teknolojileri Risk Çeşitleri

Bilgi teknolojileri kapsamında gerçekleştirilen işlem ve hizmetleri olumsuz yönde etkileyen ve bu işlemlere bağlı olarak yürütülecek olan işletme faaliyetlerinin yerine getirilmesini engelleyen faktörleri beş ana başlık altında değerlendirebiliriz.[146]

---

[144] George WESTERMAN ve Richard HUNTER, "IT Risk Turning Business Threats into Competitive Advantage", **Harvard Business School Press**, June 2007, s.1.

[145] Greg HUGHES, "IT Risk Management Report", **Symantec Corporation**, Volume 1, February 2007, s.1.

[146] TBD Kamu-BİB Kamu Bilişim Platformu 8, "Bilişim Teknolojilerinde Risk Yönetimi", **Çalışma Grubu**, 27 Mart 2006, s.4.

1) Personel riski: Bu risk kavramı, bilgi teknolojileri sistemini kullanan personelin sistem içerisinde yapmış olduğu hatalar, çalışan sorunları, eksik bilgi ve yetkinlikler nedeniyle ortaya çıkabilmektedir.

2) Teknolojik riskler: İşletme bünyesinde hatalı olarak tasarlanmış sistem mimarileri, hatalı modellemeler, güvenlik açıkları ve/veya zayıflıkları, iletişim problemleri, yazılım ve/veya donanım hataları, veri ve sistem kayıplarının oluşması durumunda ortaya çıkan risklerdir.

3) Organizasyon riski: Bilgi teknolojileri bölümü ile işletme bünyesinde operasyon işlemlerini yürüten iş kolları arasında yeterli seviyede olmayan iletişim, organizasyon, planlama ve bütçeleme hatalarına bağlı olarak; projelendirme aşamasında planlanan bütçe miktarından fazla miktarda gerçekleştirilen kaynak kullanımı sonucunda ortaya çıkan risk çeşidini ifade eder.

4) Yasal riskler: İşletmenin bilgi teknolojileri yapısında dış kaynak kullanması ve buna bağlı olarak dış kaynak kullanılan üçüncü şahıs (firma) iflasları veya anlaşmazlıkları nedeniyle oluşan riskleri ifade eder.

5) Dış riskler: İşletme bünyesinde ve/veya işletme bünyesinde olmayan ancak işletmenin bütün bilgi teknolojileri alt yapısını etkileyebilecek olan doğal afetler, sabotaj, terörist saldırılar, siber saldırılar, savaş hali, yangın, su basması gibi fiziksel tehditlerin oluşturduğu riskleri ifade eder.

Yukarıdaki belirtilen risk tanımı ve çeşitleri genel tanımlama kapsamında açıklanmış olup, organizasyonların bilgi sistemleri risklerini değerlendirmeleri, anlamaları, analiz etmeleri ve azaltma stratejilerini düzenlemeleri amacıyla organizasyona olan etkilerine göre sınıflandırılması gerekebilir. Bilgi teknolojilerine ait risk sınıflandırması aşağıdaki gibidir;[147]

---

[147] Barış BAĞCI, "Bilgi Teknolojileri Risk Yönetimine Genel Bakış", 2007, http://www.denetimnet.net/UserFiles/Documents/DeloitteMakaleleri/Bilgi%20Teknolojileri%20Risk%20Y%C3%B6netimine%20Genel%20Bak%C4%B1%C5%9F.pdf, (08.07.2013), s.8.

Güvenlik riski: İşletmenin kullandığı sistem içerisinde yer alan bilgi ve/veya veriler değiştirilebilir, erişilebilir veya yetkisiz kişilerce kullanılabilir. Bu durumda sistem içerisinde ve dışarısında yer alan güvenlik ortamının analiz edilmesi, değerlendirilmesi ve gerekiyorsa yeniden yapılandırılmaya gidilerek kontrol ortamının revize edilmesi sağlanabilir.

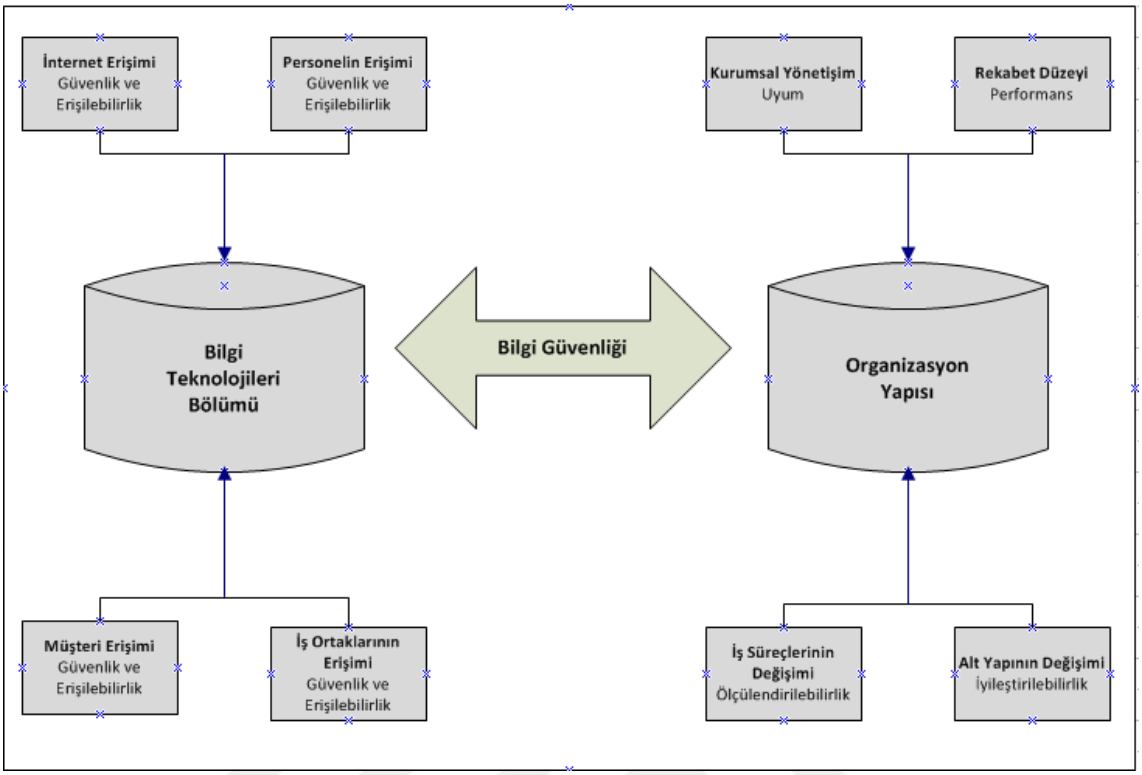
Erişilebilirlik: İşletmenin faaliyetlerini yürüttüğü sektör içerisinde karar ve strateji belirlenmesini sağlayan bilgi veya uygulamalara herhangi bir nedenden dolayı (örn. doğal afet) erişimi kısıtlanabilir ve/veya engellenebilir. Bu risk durumunun oluşması iş sürekliliği ve/veya alternatif sistem erişim çözümleri vb. uygulamalarla giderilebilir. Önemli olan bu risk faktörünün oluşması durumunda; işletme bünyesinde gerçekleştirilecek olan aksiyonlara ait iş bölümünün işletme içerisinde yapılmasının sağlanmasıdır.

Geri Kazanılabilirlik: İşletmenin kullandığı sistem içerisinde yaşanan veri kaybı ve/veya sistem veri havuzunun kullanılamaması durumunda sistem içerisinde yer alan verilerin istenilen süre içerisinde geri getirilmemesi durumu oluşabilir.

Performans riski: İşletmenin operasyonlarında kullandığı bilgi sistemleri, uygulamaları veya personelin önceden belirlenmiş olan performans kriterinin altında performans ortaya koymasına bağlı olarak iş verimliliği, üretkenliği veya değeri azalabilir.

Ölçeklenebilirlik: İşletmeye ait bilgi sistemleri yapısı, işletme içerisinde yer alan bölümlerin değişen bilgi gereksinimlerini karşılamak amacıyla geliştirilemeyebilir veya değiştirilemeyebilir.

Uyumluluk riski: İşletme bünyesinde oluşturulan bilginin muhafaza edilmesi ve işlenmesi faaliyetleri, işletme politika ve prosedürlerine, yasal gereksinimlere uygun bir şekilde yerine getirilemeyebilir.



Şekil 13: Bilgi Teknolojileri Riski Öğeleri
Kaynak: Barış BAĞCI, "Bilgi Teknolojileri Risk Yönetimine Genel Bakış", 2007, http://www.denetimnet.net/UserFiles/Documents/DeloitteMakaleleri/Bilgi%20Teknolojileri%20Risk%20Y%C3%B6netimine%20Genel%20Bak%C4%B1%C5%9F.pdf, (08.07.2013), s.8.

Yukarıdaki altı kategori içerisinde, işletmelerde maruz kalınan bilgi sistemleri risklerine ait öğeler sınıflandırılmıştır. Bu sınıflandırma içerisinde önceliklendirme yapılması mümkün olmamaktadır. Her organizasyon kendine özgü oluşturulan bilgi sistemleri ile ilgili olarak risk profiline sahip olmakla birlikte, her organizasyonun yapacağı önceliklendirme kendi iş değerlerine göre yapılmaktadır.

2.5.3 Bilgi Teknolojileri Risklerinin Operasyonel Riskler ile Bağlantısı

Stratejik bilgi kavramının ortaya çıkışı; bilgi teknolojilerinin içerisinde bulunan bilgi kavramının güncel ekonomi içerisinde işletmeler için değerinin artması ve önemli bir rekabet avantajı haline gelmesinden kaynaklanmaktadır. Stratejik bilgi; işletmenin diğer işletmelerden ayrışmasını sağlayan yüksek gizliliği olan bilgidir. Stratejik bilgi sistemleri stratejik bilgi sisteminin yönetimi olarak dikkate alınabilir. Bu nedenle bilgi sistemleri işletmeye ait iş stratejilerinin desteklenmesi amacıyla operasyonel seviyeden stratejik seviyeye taşınmıştır. Bu gelişmeye bağlı olarak iş stratejileri ile bilgi sistemleri

stratejilerinin uyumlu olması bilgi sistemlerinin ve işletmenin başarısı açısından önemlidir.[148]

Bir organizasyon yapısı içerisinde yer alan bilgi teknolojilerinin en temel görevi, bir organizasyondaki tüm yönetim kademelerine gereksinim duydukları bilgiyi sağlamaktır. İşletme yapısında görev alan yöneticilerin bulundukları pozisyon ve kademeye göre ihtiyaç duydukları bilgi miktarı ve içeriği farklılaşabilir. Bu nedenle bilgilerin yer aldığı bilgi teknolojileri, bilgileri kullanan yöneticilere farklı bilgilerin farklı formatlarda sunmaları sağlanmalıdır. İşletmelerdeki bilgi teknolojileri yapısının her organizasyonun yapısına, kurallarına, işlemlerine, amaç ve hedeflerine uygulanabilecek bir yapıda oluşturulması gereklidir. Bilgi teknolojileri yapısının sıvı bir madde olduğu düşünüldüğünde; girmiş olduğu yerin şeklini alabilme yeteneğine sahip olması gereklidir.[149]

İşletme bünyesinde müşteri odaklı olarak işletme strateji ve hedefinin müşterilere en hızlı ve en doğru servis ve çözüm desteğinin verilmesi olması durumunda, bu yapıya ait ve bu yapıyı destekleyen bilgi sistemlerinin işletme bünyesinde oluşturulması sağlanmalıdır. Bir başka örnek olarak işletme içerisinde önemli bir yere sahip olan satın alma ve tedarik süreçlerinin etkin ve verimli bir şekilde yönetilmesi, maliyetlerin düşürülmesine olanak sağlamakla birlikte, işletme bünyesinde bu hedefi ve stratejiyi destekleyecek olan tedarik zinciri yönetim bilgi sisteminin oluşturulmaması, işletme hedef ve stratejileri ile bilgi sistemlerinin uyuşmadığını göstermektedir.[150]

İşletme operasyonları ile işletme bünyesindeki üst yönetim tarafından onaylanmış olan bilgi teknolojileri risk stratejilerinin uyumlu olması, işletmelerin risklerini yönetirken ve maliyet değerlerini kontrol altına alırken ortaya çıkan ve/veya çıkabilecek olan fırsatları izlemelerine imkân sağlar. İşletme organizasyon yapısı

---

148 Ekrem EMRE ULTAV, "Bilgi Sistemlerinin İşletmeler için Stratejik Önemi ve Başarısının Ölçülmesi", **Yüksek Lisans Tezi**, İstanbul, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s.31.

149 Hakan ANAMERİÇ, "Yönetim Bilgi Sistemlerinin Yönetim Fonksiyonları Üzerine Etkisi", **Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi**, Sayı:2, 2005, s.42.

150 ULTAV EMRE, a.g.e., s.32.

içerisinde yer alan organizasyonel hedeflerle uyumlu ve bağlantılı olarak bilgi teknolojileri risk stratejileri oluşturulmalıdır. İşletme yapısı içerisinde en üst düzeyde yer alan bilgi teknolojilerine ait süreçler, işletme stratejisini desteklemelidir.[151]

İşletme içerisinde oluşturulmuş ve etkili olan bilgi teknolojilerine ait risk yönetim stratejisi, işletme süreç sahiplerinin iş hedeflerini destekleyici nitelikte olur. Risk yönetim stratejisi programı süreç sahiplerine ait risk seviyelerini dikkate alarak en alt seviyedeki risk seviyelerini kabul eder. İşletme bünyesindeki iş kollarına ait operasyonel ve bilgi teknolojileri riskleri arasındaki bağlantı değerlendirildiğinde, bilgi teknolojilerinin kullandığı varlık ve bunlara bağlı olarak gerçekleştirilen operasyonların işletme bünyesindeki faaliyetlere katkı sağladığı durumu ortaya çıkar. İşletme içerisindeki operasyonel ve bilgi teknolojileri riskleri arasındaki ilişki ve bağlantıya bağlı olarak iş kolları stratejilerine göre farklılık göstermesi, işletmenin verimliliğinin artmasına olanak sağlar.[152]

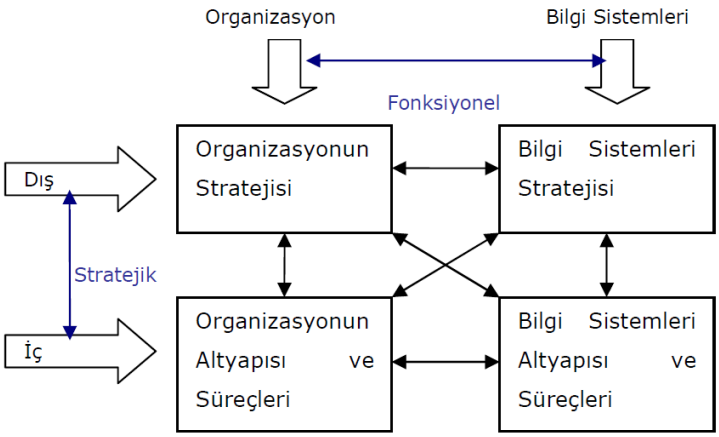
Henderson ve Venkatraman tarafından "stratejik uyum modeli" ile 1993 yılında işletme organizasyonun ve işletme bünyesinde yer alan bilgi teknolojileri sistemlerinin uyumu açıklanmaya çalışılmıştır. Bu model içerisinde; organizasyon ve bilgi teknolojileri-sistemleri uyumu, stratejik uyum ve fonksiyonel entegrasyon olmak üzere iki boyutta açıklanmıştır. Bu model kapsamında, işletme içerisindeki faaliyetler dikkate alınarak iş hedefleri sıralanmış, bilgi teknolojilerine yapılan yatırımın değerinin öneminin kavranması amaç olarak belirlenmiştir.[153]

---

[151] Tolga ÖZGÜN, "Bilişim Teknolojileri ile İşletme Stratejileri Arasındaki Uyumun Faktör Analizi Yöntemi ile Ölçülebilirliği", **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2015, s.50-53.

[152] HUGHES, a.g.m., ss.24.

[153] Rik MAES, Daan RİJSENBRİJ, Onno TRUİJENS ve Hans GOEDVOLK, "Redefining business-IT alignment through a unified framework", **Primavera Working Paper Series-Amsterdam University**, June 2000, s.5.



Şekil 14: Stratejik Uyum Modeli
Kaynak: J.C. HENDERSON and N. VENKATRAMAN, "Strategic alignment: Leveraging information technology for transforming organizations", **IBM Systems Journal**, Vol: 32, no:1, 1993, s.8.

Stratejik uyumun kapsamı ve genişliği iki faktör tarafından belirlenmektedir. Bunlar dış ortam tarafından oluşturulan dış çevre ve iç ortam tarafından oluşturulan idare yapısıdır. Bu kriterlerden başka fonksiyonel entegrasyon kriteri organizasyon ile bilgi sistemlerini birbirinden ayırmayı sağlar. Model bir bütün olarak ele alındığında; organizasyon ile bilgi sistemleri arasındaki uyum için **4** unsurun birbiri ile uyumlu hale getirilmesi gerektiğini belirtmektedir.

Yukarıdaki şekilde belirtilen stratejik uyum yaklaşımı ile birlikte söz konusu işletme bünyesinde yer alan operasyonel faaliyetlere bağlı oluşan ve/veya bilgi teknolojilerinde yer alan süreçlere bağlı olarak oluşan riskler direkt olarak birbirlerini etkiler. Söz konusu risklerin giderilmemesi ve/veya birlikte değerlendirilmemesi; işletmenin belirlenen stratejilere ve hedeflere ulaşmasını olumsuz yönde etkileyecektir.

BDDK tarafından bankacılık sektöründeki operasyonel risk tanımı yapılmıştır. Bu tanım içerisinde risk, banka içerisinde gerçekleştirilen kontrol faaliyetlerinde oluşan aksaklıklar nedeniyle oluşan hata ve hilelerin tespit edilememesi, banka yönetimi ve personeli tarafından güncel duruma uygun hareket edilememesi, banka yönetimi tarafından gerçekleştirilen hatalı işlemlerden, bilgi teknolojisi sistemlerindeki hata ve aksamalar ile deprem, yangın ve sel gibi felaketlerden veya terör saldırılarından kaynaklanabilecek zarar olasılığı olarak tanımlanmıştır. Basel komitesi tarafından

operasyonel riske bağlı olarak oluşan kayıplara ait olay çeşitleri **yedi başlık** içerisinde belirtilmiştir. Bu başlıklardaki risk tanımı; "İşin kesintiye uğraması ve sistem arızaları; işin kesintiye uğramasından ve sistem arızalarından kaynaklanan zararlar" olarak tanımlanmıştır.[154]

Basel Komitesi, operasyonel riski, "yetersiz veya başarısız dahili süreçler, insanlar ve sistemlerden veya harici olaylardan kaynaklanan kayıp riski" olarak tanımlamıştır. Basel Komitesi tarafından operasyonel riske neden olan unsurlar; insan, sistem, süreç ve dışsal faktörler olmak üzere **dört ana** başlık altında incelenmiştir.[155]

Gelişen teknolojiye bağlı olarak mevcut durumda bankacılık sektöründe yer alan bütün iş akışlarında bilgi teknolojileri sistemleri kullanılmaktadır. Banka bünyesinde gerçekleştirilen işlem sonuçlarına ait kayıtlar, raporlamalar, karar alma işlemleri, onay ve yetki kontrolleri gibi birçok işlem banka içerisinde yer alan programlar aracılığıyla gerçekleştirilmektedir. Bu açıdan değerlendirildiğinde; bankalar için büyük öneme sahip olan bilgi sistemlerine ait riskler bankalar için önemli bir durum almıştır. Otomatik olarak yürütülmeyen faaliyetlerin, otomasyon işlemi için gerçekleştirilen ve geliştirilen yatırımlar bankalar açısından bir risk faktörü ortaya çıkarmaktadır. Bankanın süreçleri içerisinde yer alan ihtiyaçlar dikkate alınarak oluşturulan ve/veya geliştirilen sistemlerin test edilmesi ve uygulanması kapsamında bankalar önemli risklerle karşılaşmaktadır. Test işlemleri kapsamında otomatik hale getirilmeye çalışılan ve manuel işleme izin verilmeyen süreçlerin oluşturulması aşamasında yaşanabilecek olan durumlar, örneğin; sistem kesintileri, arıza ve hataların oluşması durumunda ortaya maddi zararlar çıkabilir.[156]

Basel komitesi tarafından ölçüm yaklaşımları kapsamında; operasyonel risk kayıp olay türleri toplu olarak değerlendirilmektedir. "Banka İçi Hile ve Dolandırıcılık", "Faaliyetin Durması ve Sistem Hataları", İcra, Teslimat ve Süreç Yönetimi" olay

---

[154] Ertuğrul UMUT UYSAL, "Operasyonel Risk Yönetiminde Senaryo Analizi", **Bankacılar Dergisi**, Sayı:69, 2009, s.74.

[155] Ömer KARA, "Bankalarda Operasyonel Risk", **Yüksek Lisans Tezi**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, Haziran 2009, s.3.

[156] KARA, a.g.e., s.5.

tanımlamalarında bilgi sistemleri ve operasyonel risklerin bağlantısı aşağıdaki tablodaki gibidir.

Tablo 1: Operasyonel ve Bilgi Teknolojileri Risklerinin Bağlantısı

Olay Tipi Sınıflandırması (1.Seviye)	Tanım	Olay Tipi Sınıflandırması (2. Seviye)	Faaliyet Örnekleri (3.Seviye)
Banka İçi Hile ve Dolandırıcılık	Banka içinden en az bir tarafın içine karıştığı ve söz konusu taraf veya tarafların dolandırıcılık; zimmetine geçirme; düzenlemeleri, kanunları yada şirket politikalarını dolanma veya ayrımcılık olayları şeklindeki faaliyetleri sonucu ortaya çıkan kaybı ifade eder.	Yetkisiz İşlem	Raporlanmayan işlemler (kasıtlı)
			Yetkisiz işlem tipi (mali kayba neden olan)
			Yanlış belirlenen pozisyonlar (kasıtlı)
Banka İçi Hile ve Dolandırıcılık	Üçüncü Kişilerin dolandırıcılık, zimmetine para geçirme ya da kanunları dolanmak şeklindeki faaliyetleri sonucu ortya çıkan kaybı ifade eder.	Sistem Güvenliği	Hacking Zararı
			Bilgi Hırsızlığı (mali kayıpla sonuçlanan)
Faaliyetin Durması ve Sistem Hataları	Faaliyetlerin durması, kesilmesi yada sistem hataları sonucu ortaya çıkan kaybı ifade eder.	Sistemler	Donanım
			Yazılım
			Telekominikasyon Hizmetleri
			Kamu hizmetlerinin durması / kesilmesi
İcra, Teslimat ve Süreç Yönetimi	Başarısız süreçler ya da başarısız süreç yönetimi ile ticari muhataplarla ve satıcılarla ilişkiler sonucu ortaya çıkan kaybı ifade eder.	İşlemlere ilişkin bilgilerin tutulması, işlemlerin gerçekleştirilmesi ve işlem bilgilerinin muhafaza edilmesi	İletişimin sağlanamaması
			Bilgi girilmesi, bilgi muhafazası ya da bilgi yükleme hatası
			Modelin ya da sistemin yanlış çalıştırılması
			Referans bilgi muhafazası
		Müşteri Hesaplarının Yönetimi	Hesaplara onaysız girişler
			Yanlış müşteri kayıtları

Kaynak: Murat MAZIBAŞ, ”Operasyonel Riske Basel Yaklaşımı: Risk Verilerine İlişkin Bir Değerlendirme”, **BDDK Araştırma Raporları**, Temmuz 2005, s.13-17.

Yukarıdaki tablo içerisinde bilgi teknolojileri ve operasyonel riskler arasındaki ilişki genel olarak belirtilmiş olup, bankalar bünyesinde yürütülen iş süreçlerindeki ana süreçler ve alt süreçler değerlendirildiğinde; söz konusu iki risk türü arasındaki ilişkinin kuvvetli ve/veya zayıf olduğu faaliyetlerin bulunduğu görülmektedir. Söz konusu bu ilişkinin kuvvetli ve/veya zayıf olması söz konusu süreç(ler) içerisinde yürütülen faaliyetlerdeki bilgi teknolojilerinin kullanım oranı ile ilişkili olmaktadır. Bankacılık sektöründeki faaliyetlerde bilgi teknolojilerinin yoğunluklu olarak kullanılması, süreç bazında operasyonel ve bilgi teknolojileri risklerinin bağlantılarının artmasına neden olmuştur.

2.6 Bankalarda Risk Değerlendirme Metodolojisi

2.6.1 Risk Belirleme Süreci

İşletme riskinin tanınması ve ölçülmesi işlemleri mevcut durum içerisinde herhangi bir değişikliğe neden olmamakla birlikte; işletme faaliyetlerinde oluşabilecek olan olumlu ve/veya olumsuz sonuçları bilinir hale getirmemektedir. Bir işletme içerisinde yer alan risk kavramı belirlenip, hesaplanmasına rağmen işletme içerisindeki faaliyetlere ait operasyon sonuçlarının başarısız olma ihtimalini ortadan kaldırmamaktadır. Risklerin belirlenmesi, tespit edilmesi işletme bünyesinde mevcut durumda ve ileriye yönelik alınacak olan kararlar ve gerçekleştirecekleri işlemler konusunda daha sağlıklı karar verebilmelerini sağlar. İşletme bünyesinde risk kavramı, mevcut durumu net bir şekilde görüntülemeye engel olan, yöneticileri yanlış ve/veya hatalı olarak karar almaya yönlendiren bir durum olarak algılanması durumunda, riskin belirlenmesi ve hesaplanması sağlanarak, bu algının farklı bir alana yönlenmesi sağlanabilir. Bu durumda işletme bünyesinde risk kavramına karşı bakış açısı değişmekle birlikte belirsizlik durumunun ortadan kalkmasına olanak sağlayabilir.

İşletme bünyesinde risklerin belirlenmesi işlemi üç aşamadan oluşmaktadır. Bu aşamalar;

a) Riskin Tanımlanması: Risk tanımlaması, işletmenin belirsizliğe maruz kalmasını belirlemektir. Risk tanımlaması işletme ile ilgili olan özel bilgileri içerir. İşletmeye ait olan bilgiler; işletmenin içerisinde yer aldığı sektör ve/veya sektörler, yasal, politik, sosyal ve kültürel çevrelerden oluşmaktadır. Bu bilgilere ek olarak işletmeye özgü olan stratejik ve operasyonel hedefler ve bu hedeflerle ilgili olan fırsat ve tehditlerinde dikkate alınması ve net bir şekilde anlaşılması gereklidir.

Risk tanımlamasının ilk aşamasında işletme için riskli olduğu tespit edilen önemli değişkenlerin etkisi ve içeriği konusundaki belirsizliklerin minimize edilmesine odaklanılmaktadır. Belirsizliklerin azaltılmasına ve/veya çözülmesine katkı sağlayacak olan bilgi kaynağının ve işlemlerin daha iyi bir şekilde belirlenmesi gereklidir. Bu işlemlerin tam, doğru ve zamanında yapılabilmesi amacıyla geleceğe yönelik olarak planlama araç ve gereçleri kullanılabilir. Bu yapıda bir planlamaya örnek olarak,

işletmenin gelecekte karşılaşabileceği fırsat ve kayıpları tespit edebilmek amacıyla geleceğe ilişkin senaryolar oluşturulur.[157] Oluşturulan senaryolara ait çeşitli olay tanımlamaları yapılır. Oluşturulan araç ve yöntemler, değişkenlerin ve belirsiz etkilerin yönetim tarafından anlaşılmasını ve benimsenmesini kolaylaştırabilir.[158]

Risk tanımlaması, işletmenin içerisinde yer alan önemli faaliyetlerin tanımlanmasını ve bütün risklerin bu tanımlanan faaliyetlerin süzgecinden geçirilmesini sağlar. Bu nedenle işletme bünyesinde faaliyetlerle ilgili gerçekleştirilen değişiklikler tam, doğru ve zamanında tanımlanmalı ve sınıflandırılmalıdır.

İşletme faaliyetleri ve kararları, aşağıda belirtilen örnekler dahilinde sınıflandırılabilir;

- **Stratejik:** Bu kavram; işletme organizasyonun uzun dönem içerisinde hedeflemiş olduğu uzun dönem olan stratejik hedefleriyle ilgilidir. Mevcut durum şartlarına göre belirlenen stratejik hedefler, sermayenin kullanılırlığı, politik riskler, yasal mevzuattaki değişikliklerden ve fiziksel çevre değişikliği gibi faktörlerden etkilenebilir. Etkilenme sonucunda, işletme tarafından hedeflerde değişikliklere ve/veya revize yapmaya ihtiyaç duyulabilir.

- **Operasyonel:** İşletmenin stratejik hedeflerini sunma yeteneğine ve sunma gayretiyle ve günlük olarak bu sunma yeteneğini ve gayretini nasıl yerine getirebileceğine bağlıdır.

- **Finansal:** İşletme içerisinde yer alan finans bölümüne ait organizasyon yapısının etkin yönetimi ve kontrolü ile dış faktörlerin (kredilerin kullanımı, kurlar ve faiz oranlarındaki hareketler ve diğer pazar kayıpları vb.) etkilerinden oluşmaktadır.

- **Bilgi Yönetimi:** Bilgi yönetimi, işletme içerisindeki bilgi kaynaklarının efektif yönetilmesi ve kontrol işlemleri ile ilişkilidir. Bilgi yönetimine ait dış faktörler;

---

[157] Selda ENE, " Proje Yönetiminde Yer Alabilecek Risk Kaynaklarının Tespiti ve Risk Yönetim Planının Geliştirilmesi", **İstanbul Sosyal Bilimler Dergisi**, Sayı:5, 2013, s.55.

[158] BAŞARIR, a.g.e., s.5.

rekabetçi teknolojik ortamlardan, iç faktörler ise sistem arıza ve bozukluklarından veya anahtar kullanıcı personelin kayıp edilmesinden oluşur.

- **Uyum:** Uyum kavramı, işletme bünyesinde sağlık ve güvenlik koşullarının sağlanması, faaliyetlere ait iş tanımlamalarının oluşturulmasının yanı sıra müşterinin ve müşteri verisinin korunması, yasal kriterler gibi konuları içermektedir.

İşletme bünyesinde yer almayan dışardan danışmanlık hizmeti veren danışmanlar tarafından risk tanımlanması yapılabilir. İşletme bünyesinde yer almayan bağımsız bir danışman tarafından yapılacak olan risk tanımlamasının başarısı, işletme yaklaşımının iyi iletişim ve yeniden oryante edilmiş işlem ve araçlarının kullanımına bağlıdır. Risk yönetimi işlemlerine ait en öncelikli ve en önemli konu "bir kurum olarak sahiplenme" yaklaşımına sahip olmaktır.

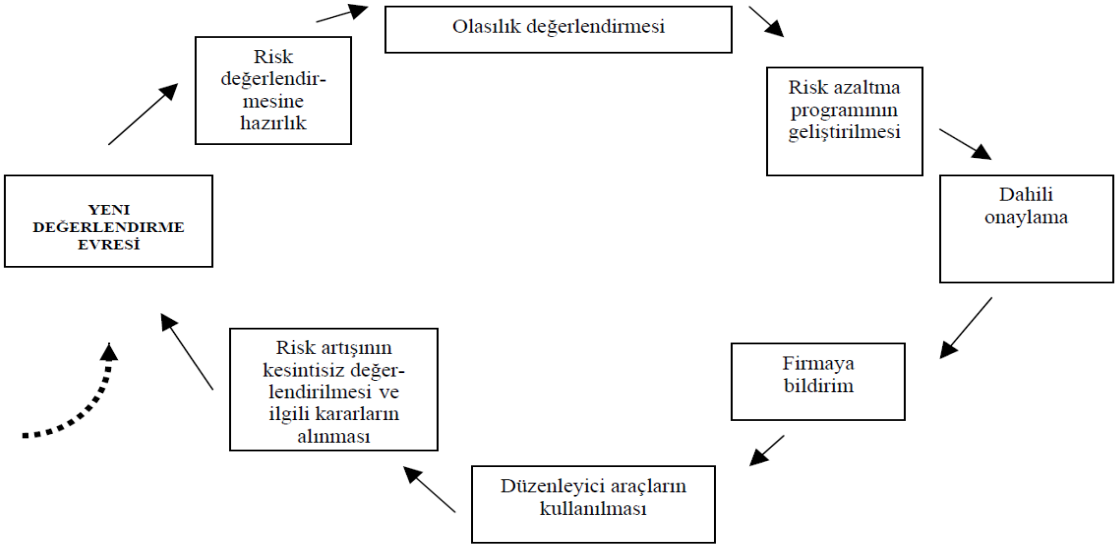
b) Riskin Ölçülmesi: Riskin ölçülmesinin amacı, işletmelerin gerçekleştirmiş olduğu faaliyetlerinden oluşan risklerin tek başlarına hangi risk sınıfı ve kategorisine gireceğini belirlemek ve ona göre karar alıp, aksiyon planının oluşturulması sağlanmalıdır.

c) Riskin Değerlendirilmesi: Risk tanımı yapılan ve ölçümlenen riskin işletme bünyesinde değerlendirilmesi yapılır. Risk değerlendirme işleminde tanımlanan ve sınıflanan risklerin işletme bünyesindeki kabul edilebilir ve/veya kabul edilemez olup olmadığı durumu gözden geçirilir. Risk değerlendirilmesi aşaması aşağıdaki bölüm içerisinde ayrı olarak aktarılacaktır.

2.6.2 Risk Değerlendirme Metodolojisi ve Yaklaşımı

Risk değerlendirme çerçevesi; birden fazla aşamadan oluşmaktadır. Söz konusu bu yapısal aşama kapsamında, işletmeye ait risklerin azaltılmasını sağlayacak olan bir program üzerinde yoğunlaşmaktadır. Aşağıdaki şekil içerisinde belirtilen aşamalar risk değerlendirme çerçevesinin 9 adet temel özelliği bulunduğunu göstermektedir.[159]

[159] Türkiye Bankalar Birliği, "Finansal Kurumlar İçin Risk Değerlendirme Çerçevesi", Ocak 2004, s.7.



Şekil 15: Risk Değerlendirme Çerçevesi
Kaynak: Türkiye Bankalar Birliği, "Finansal Kurumlar için Risk Değerlendirme Çerçevesi", Ocak 2004, s.7-8.

Yukarıdaki şekilde yer alan bilgiler değerlendirildiğinde, risk değerlendirme bir süreçtir. Risk değerlendirme işleminde işletme bünyesinde kullanılan bir sistem içerisinde oluşacak olan tehlike ve tehditlerden kaynaklanan risklerin büyüklüğü belirlenir. Büyüklüğü belirlenen risklerin işletme içerisinde yer alan mevcut kontrollerle minimize edilip edilemeyeceği analiz edilir. Mevcut durumda işletme bünyesinde yer alan kontrollerin yeterliliği değerlendirilerek, risklerin kabul edilebilir olup olmadığına karar verilir. Risk değerlendirme teknikleri birden fazladır. Risk değerlendirme teknikleri, risklerin gerçekleşme olasılıklarının ve olası etkilerinin tahmin edilmesi açısından iki ana grupta toplanabilir. Bunlar, kalitatif ve kantitatif yöntemlerdir.[160]

Kalitatif yöntemlerde, matematiksel risk değerlendirmesi yerine sözel mantık kullanılarak risk değerlendirmesi yapılır. Risk, sistematik veya sistematik olmayan şekilde sübjektif ve risk değerlendirmesi yapanın tecrübelerine ve sezgilerine dayanmaktadır. Risk değerlendirmesinde kalitatif yöntemin kullanılırken öncelikle "Anahtar Risk Göstergeleri" belirlenir. Anahtar risk göstergelerine göre risk nedenlerinin

[160] Hüseyin CEYLAN ve Volkan S. BAŞHELVACI, "Risk Değerlendirme Tablosu Yöntemi ile Risk Analiz: Bir Uygulama", **International Journal of Engineering Research and Development**, Cilt 3, Sayı 2, Haziran 2011, s.26.

oluşması konusunda tahmin yapılmaya çalışılır. Risk nedenleri tahmin edildikten sonra fayda-maliyet analizi yapılarak risk değerlendirmesi yapılır. Tahmini risk miktarının hesaplanmasında ve tanımlanmasında düşük, orta, yüksek, kritik vb. değerlere yer verilir. Kalitatif risk değerlendirme yönteminde risk miktarı hesaplanmasında ve tanımlanmasında sayısal bilgi ve değerler kullanılmamaktadır.[161]

Kantitatif risk değerlendirme yöntemleri, riski hesaplarken sayısal yöntemleri ve değerleri kullanır. Bu yöntem içerisinde, basit istatistiki modeller, olasılık ve güvenirlik teorileri kullanılabilir. Söz konusu yöntem içerisinde ayrıca simülasyon modellerine dayalı olan karmaşık yöntem ve teknikler de kullanılabilir. Bu yöntem içerisinde ortaya çıkan olay sayısı ve işlemenin karşılaşacağı muhtemel zarar miktarı dikkate alınarak değerlendirme yapılır.[162]

Kantitatif risk analizi kapsamında tehlikeli bir olayın meydana gelme ihtimali, tehlikenin etkisi gibi değerlere sayısal değerler verilir. Belirlenen değerler kullanılarak matematiksel hesaplama ile risk değeri hesaplanır.

Risk = Tehlikeli Bir Olayın Meydana Gelme İhtimali * Tehlikenin Etkisi

formülü kantitatif risk analizinin temel formülüdür.[163]

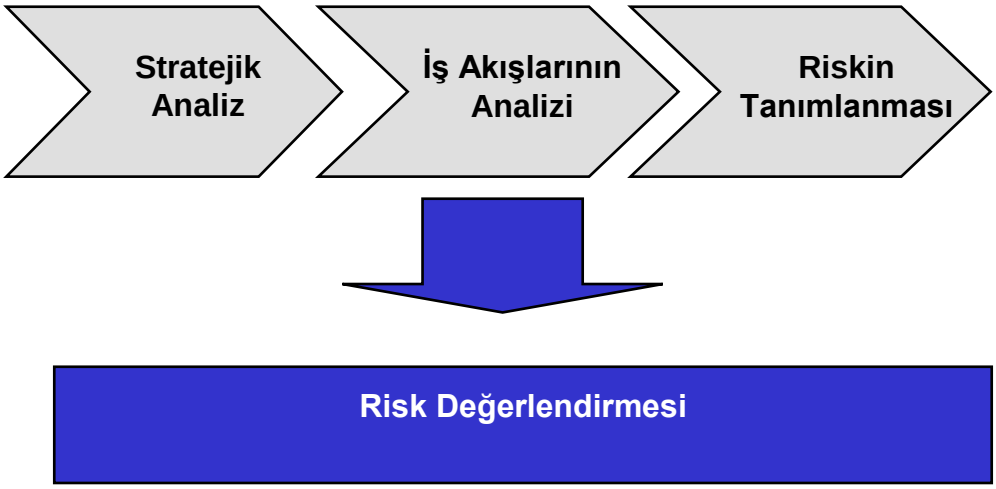
Risk değerlendirme işlemi gerçekleştirilmeden önce işletmeye ait oluşturulmuş olan süreçler içerisinde yer alacak bölümlerin belirlenmesi için anahtar stratejik, operasyonel, finansal raporlama gibi aşamaların belirlenmesi gereklidir. Bu aşamaları özetlemek gerekirsek,

---

[161] ÖZÇELİK, a.g.e., s.82.

[162] Artur ROT, "IT Risk Assesment: Quantitative and Qualitative Approach", **Proceedings of the World Congress on Engineering and Computer Science**, 22-24 Ekim 2008, San Francisco, USA, s.2.

[163] CEYLAN ve BAŞHELVACI, a.g.m., ss.27.



Şekil 16: Risk Değerlendirme Süreci

Risk değerlendirme işleminin hedefleri;

- İşletmeye ait operasyonel fonksiyonların eksiksiz olarak yönetilmesi
- İşletmeye ait operasyonel ve anahtar stratejik değişikliklerdeki önemli değişikliklerin belirlenmesi
- Anahtar iş risklerinin belirlenmesi
- Tanımlanan risklerin ölçülmesi ve öncelikli olanların belirlenmesidir.

Yukarıdaki hedeflerin yerine getirilebilmesi için işletmeye ait operasyonel faaliyetlerinin iyi tanımlanması ve bu tanımlamalar dikkate alınarak, iş akışlarının analizlerinin yapılması ve risk tanımlamalarının oluşturulması gereklidir. Risk tanımlamaları yapıldıktan sonra oluşturulan risk tanımlamalarının etki derecesi dikkate alınarak risk matrisi oluşturulur.

2.6.3 Risk Matrisi-Kontrol Kataloğu İçeriğinin Oluşturulması

Risk matrisi; bir bankanın stratejik hedeflerine göre öncelikli faaliyet olarak tanımladığı ve söz konusu bu faaliyetlerde karşılaştığı risk çeşitlerini ve seviyelerini ölçer. Risk matrisi uygulaması risk yönetimi uygulamaları sonucunda azaltılan risk bakiyelerini de ölçer. Risk matrisi uygulaması, risk yönetimini bir sistem olarak dikkate

almakla birlikte; münferit olarak tanımlanan risklerin yönetimine bağlı olarak ortaya çıkan sonuçların da kontrol edilmesine olanak sağlar.[164]

Bankacılık sektöründe risk matrisi; bankaların işlevsel faaliyetlerinin, bu faaliyetlerle bütünleşik risklerinin türünün, seviyesinin ve gelişim yönü ile bu faaliyet alanlarındaki risk yönetim sistemlerinin yeterliliğiyle birlikte her bir faaliyet bazında ve bankanın tamamı için **Net Risk**[165] seviyesinin ve gelişim yönünün tespiti için kullanılan bir analiz yöntemidir. Risk matrisi, bankanın her bir faaliyet bazında risk profilini, risk yönetim sistemlerinin etkinliğini, net riskin seviyesini ve bankanın risk profilindeki değişimleri gösteren esnek ve dinamik bir analiz aracıdır.[166]

Risk matrisi işletmeye ait risk tanımlamaları dikkate alınarak oluşturulur ve geliştirilir. Risk matrisi, işletme yöneticilerinin ve yönetim kurulunda görev alan yönetim kurulu üyelerinin, çeşitli risk sınıflandırılmasında gruplandırılan risk tanımlamalarının etkin ve verimli bir şekilde anlaşılmasını sağlar.

Risk matrisi, bankacılık başta olmak üzere finans sektöründe kredi riski, döviz kurları ve emtia fiyatları ile ilgili alanlarda kullanılmaktadır.[167]

Risk değerleme metodolojisi olarak genellikle; geniş kapsamlı olarak iş riski değerleme metodolojisi (Comprehensive Business Risk Assessment (CBRA)) kullanılmaktadır. Bu metodoloji, sistematik ve bütünsel olarak riskleri ve fırsatları gözden geçirir. Risk değerleme metodolojisi, işletmenin risklerini yönetim için bir girdi olarak tanımlar ve öncelik sırasına göre sıralandırır. Bu metodoloji ayrıca işletmenin risklerini ortaya çıkarmak için destekleyici dokümanları gözden geçirerek, iç denetim planının ve programının oluşturulmasını sağlar.

---

[164] Ahmet YARIZ, "Bankacılıkta Risk Yönetimi: Risk Matrisi Uygulaması", **Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü E-Dergisi**, Sayı 1, Temmuz 2011, s.1.

[165] **Net Risk**, bankaların işlevsel faaliyetleriyle bütünleşik risklerin (finansal ve finansal olmayan riskler) seviyelerinin risk yönetim ve kontrol sistemlerinin etkin çalışması suretiyle azaltılmasının ardından kalan risk miktarıdır. Net Risk kavramı, "bütünleşik ortalama risk düzeyi" kavramı ile aynı anlama gelecek şekilde kullanılmıştır.

[166] YARIZ, a.g.m., ss.1.

[167] YARIZ, a.g.m., ss.5.

Şekil 17: Geniş Kapsamlı İş Riski Değerleme Metodolojisinin İçerikleri

İş riski değerlendirme metodolojisi, işletme yönetimine hangi önemli iş risklerine odaklanması gerektiğini gösterir. Odaklanması gereken iş risklerinde yer alan fırsatları tanımlayarak, işletmenin amaç ve hedeflerine ulaşmasında işletme yönetimine yardım eder. İş riski değerlendirme metodolojisi toplam 4 aşamadan oluşur. Bu aşamalar sırasıyla;

1) Stratejik analiz,

2) İş süreci analizi,

3) Risk analizi,

4) Planlama,

1) Stratejik Analiz: Yapılacak olan stratejik analizin öncelikli ve temel hedefi, organizasyonun önemli iş süreçlerinin tespit edilmesi ve bu iş süreçlerine ait olan riskleri belirlemektedir. Bu nedenle aşağıdaki yer alan işlemler sırasıyla gerçekleştirilir;

- İş akışlarından sorumlu olan yöneticilerle ve iş süreçlerini gerçekleştiren çalışanlarla görüşme yapılması,

- Önemli iş akışları ile ilgili iç kontrol faaliyetlerine ait işletmenin oluşturduğu dokümantasyonların gözden geçirilmesi,

Süreç sahipleri ile yapılan görüşmeler, yönetimin aşağıda belirtilen alanlarla ilgili olarak yönetim bakış açışını anlamak açısından önemlidir.

- Söz konusu iş sürecini gerçekleştiren bölüme ait stratejik hedefler ve bu hedeflerin kurumun amaçlarına ulaşılmasındaki rolü,

- Riskin minimize edilmesinde kullanılan kontroller göz önüne alınarak departmanın amaçlarına ulaşması,

- Riskleri minimize etmek amacıyla kullanılan kontrollerin hedeflere ulaşılmasındaki rolü,

- Performans ölçütleri ve göstergeleri,

- Stratejik hedeflere ulaşırken karşılaşılan engeller,

- Geliştirilecek olan alanlar,

2) İş Süreci Analizi: İş süreci analizi işletmenin; önemli iş süreçlerinde yer alan risklerini öncelik sırasına göre sıralandırır. Bu analiz, süreci analiz eden kişinin deneyimine ve yönetimle yapılan görüşmelerin sonucuna göre geliştirilir. Risk seviyesi, işletmenin faaliyetlerini gerçekleştirdiği, faaliyet çevresini içerik yönünden değerlendirir. İş riski değerlendirme metodolojisi, işletmenin maruz kaldığı içsel ve dışsal risk faktörlerini tanımlar.

3) Risklerin Analizi: Bu süreç içerisinde işletme için tanımlanmış ve belirlemiş olan risklerin önceliklerini, ortaya çıkma ihtimallerini, oluşturacakları kayıpların büyüklüğü ve zaman aralıkları derecelendirilmekte; riskten etkilenecek olan unsurlar

tanımlanarak risk matrisi oluşturulmaktadır. Oluşturulan matris kapsamında risk toleransları belirlenir ve risk puanları oluşturularak alternatif planlar hazırlanır.[168]

4) Planlama: Bu aşama içerisinde, işletme tarafından belirlenen risklerin azaltılması için acil durum planı ve risk yönetim planı hazırlanır.

2.6.4 Risk Değerlendirme Metodolojisinde Kontrol Kataloğunun Rolü

Banka bünyesinde ve/veya işletme bünyesinde yürütülen işlemlerle ilgili olarak oluşan risklerin belirlenmesi ve yönetilmesi amacıyla oluşturulan risk kontrol matrisleri, genellikle operasyonel risklerin önlenmesine katkı sağlar. Operasyonel riskler personel, teknolojik, organizasyonel, yasal ve dış risklerden oluşur. Operasyonel riskler farklı seviyelerde oluşur. Operasyonel risklerin içerisinde yer alan bu riskler[169]:

a) Personel Riski: Banka bünyesinde görev alan üst yönetimin ve çalışan personelin yürüttüğü işlemleri ve faaliyetleri etkin ve verimli bir şekilde yerine getirmemesinden kaynaklanan riskleri ifade eder. Personel riskine örnek olarak, banka yönetiminin belirlemiş olduğu onay limitlerinin üzerinde ve belirlenen kriterlerde kredi güvence bedeli temin edilmeden müşterilere kredi limitlerinin açılması durumu örnek olarak gösterilebilir. Bunun yanında yeni teknolojik gelişmelere bağlı olarak yeni teknoloji uygulamalarının banka bünyesinde dahil edilememesi, buna bağlı olarak kontrol ortamının zayıflaması ve/veya yeni teknolojik alt yapıya, mevcut personelin katkı verememesi, personelin yolsuzluk ve sahtekarlık işlemlerinde görev alması ve banka bünyesinde oluşturulan kurallara aykırı olarak hareket etmesi personel riski tanımlamasına dahil olmaktadır. Personel riskine sebep olan temel nedenler, personelin bilgi ve tecrübe yetersizliği, personelin düzensiz yer değişimi ve çalıştığı alanın elverişsizliğinden kaynaklanabilir.

---

[168] YARIZ, a.g.m., ss.5.

[169] Melek Acar BOYACIOĞLU,"Operasyonel Risk Yönetimi", **Bankacılar Dergisi**, Sayı:43, 2002, s.52.

b) Teknolojik Riskler: Bankanın kullanmış olduğu teknik alt yapı ve donanımlarda oluşan teknik aksaklıklar ve problemler, yeterliliğini kaybetmiş ve revize edilmesi gereken sistemlere bağlı olarak oluşan riskleri ifade eder.

c) Organizasyon Riski: Banka organizasyon yapısı ve yapı içerisinde gerçekleştirilen faaliyetlere bağlı olarak oluşan problemlerden ortaya çıkan riskleri ifade eder. Örneğin, organizasyon içerisindeki pozisyonlar ve bölümler arasındaki bilgi akışı yetersizliği, pozisyona ve/veya kullanıcıya bağlı olarak yetki kısıtlamalarının kesin çizgilerle belirlenmemesi organizasyon riskinin oluşmasına neden olabilir.

Organizasyon riski, içerisinde iş faaliyetlerine ait süreç ve işleyiş risklerini içerir. Süreç ve işleyiş riskleri;[170]

- Karar verme, izleme ve raporlama için uygun olmayan prosedürleri ve kontrol işlemlerini,
- Organizasyonel eksiklikleri ve yetersizlikleri,
- İşletmeye/bankaya ait bilgilerin uygun olmayan prosedürlere göre işlenmesini, (örneğin mali kayıtların oluşturulmasında oluşan hata ve/veya yanlışlıkların kayıt belgelerinin incelenerek düzeltilmemesi.)
- Risk izleme ve risk aşımları: Yönetimin riskleri izlemesindeki eksiklikler ve/veya yetersizlikler, işletme ve/veya banka bünyesinde doğru risk raporlamasını teşvik edecek olan prosedür ve/veya uygulama talimatlarının bulunmamasını,
- İşlemlere ait kayıt bilgilerinin hatalı ve/veya yanlış olarak işletme kayıtlara alınmasını,
- Bilgi sistemlerinin ve/veya risk ölçümlerindeki teknik yetersizlikleri kapsar.

[170] Joel BESSIS, **Risk Management in Banking**, 2. Baskı, İngiltere: John Wiley&Sons Ltd., 2002, s.21.

d) Yasal Riskler: Bankalar faaliyet gösterdikleri alanda yenilenmiş ve/veya çeşitlendirilmiş olan işlemleri uygulamaya çalışırken (örn. yeni kredi ürününün banka bünyesinde uygulanmaya başlanması) girerken veya uluslararası bankacılık faaliyetlerini gerçekleştirirken yasal risklerle karşılaşabilirler.

e) Dış Riskler: Banka bünyesinde gerçekleştirilen işlemler dışında üçüncü kişilerle ilgili ortaya çıkan hile ve/veya suiistimal işlemleri, risk doğurması muhtemel konularla ilgili olan hukuki düzenlemelere ait değişiklik ve boşluklar, doğal afetlerden kaynaklanan riskler vb. dış riskler grubuna girmektedir.

Operasyonel risk ile ilişkili olan diğer risk çeşitleri dikkate alındığında, banka ve/veya işletmeye ait süreçler kapsamında risk matrislerinin oluşturulması, söz konusu bu risk çeşitlerinin tanımlanarak, gelişen koşullara ve konuma göre revize edilmesini ve risklerin işletme ve/veya banka bünyesinde minimize edilmesini sağlar.

Bu yöntem içerisinde işletme yapısında yer alan bölümler, organizasyon fonksiyonları veya iş akışları risk çeşitlerine göre risk matrisi içerisinde sınıflandırılır. Bu uygulama, bankanın zayıf olduğu faaliyet alanlarını ortaya çıkartabilir. Bankanın zayıf olduğu faaliyet alanları ile ilgili olarak banka yönetimi tarafından alınacak olan aksiyonların, önlem ve faaliyetlerin uygulanma sırası yapılan çalışmaların sonuçlarına göre değerlendirilir. Risk matrisinin kapsamı genişletilerek, banka şubeleri, belirlenmiş bölgeler ya da organizasyon yapısındaki iş kollarının operasyonel risk düzeyleri derecelendirilebilir.

İş kollarına ait risk düzey derecelerinin hesaplanmasında[171];

- İşletme içerisinde görev alan çalışanların operasyonel risk seviyesi ve kontrol etkinliği ile ilgili değerlendirmeleri,
- Anahtar risk göstergeleri ve kayıp veri tabanından elde edilen veriler,

[171] UMUT UYSAL, a.g.m., ss.77.

operasyonel risk yönetimi bölümleri tarafından, belirli periyotlarda, çeşitli yöntemler kullanılarak değerlendirme kapsamına dahil edilir. Risk matrisi kapsamında elde edilen sonuçlar, risk odaklı denetim planlamasında önemli bir girdi olarak kullanılır.

2.7 Bankalarda Risk Yönetimi

2.7.1 Türk Bankacılık Sektöründe Risk Yönetimi

Geçmiş dönemlerde yaşanan ekonomik krizler, reel sektör ile finans sektörünün iç içe olduğunu bir kez daha belirgin bir şekilde göstermiştir. Ülkemizde ve dünyada yaşanan ekonomik krizler neticesinde, bankacılık sektöründe faaliyet gösteren bankaların birçoğunun TMSF (Tasarruf Mevduatı Sigorta Fonu)'na aktarılmasına neden olmakla birlikte, dikkatlerin finans sektörü üzerinde yoğunlaşmasına neden olmuş ve yaşanan krizler ile birlikte finans piyasasında risk yönetiminin önemi daha net anlaşılmıştır.

Türk bankacılık sektöründe 1990 döneminin sonlarına doğru bankalar kanununda ortaya çıkan değişimler dikkat çekmektedir. 1999 dönemi içerisinde 4389 sayılı kanun yerine 4491 sayılı bankacılık kanunu oluşturulmuştur. Bankalar kanununda meydana gelen en önemli değişiklik, bankaların finansal pozisyonlarının ve bankacılık sistemlerinin gözetim ve denetiminin güçlendirilmesi konusunda olmuştur. 4389 sayılı kanun yerine oluşturulan 4491 sayılı kanun, uluslararası en uygulamalar dikkate alınarak hazırlanmıştır. Bankalar kanunu ile mali sistemin güven ve istikrarını sağlama amacına yönelik olarak ülkemizdeki banka denetim ve gözetimin etkinliğinin artırılması ile birlikte, uluslararası standartlara uyum sağlanmıştır. 4491 sayılı yeni Bankalar Kanunu içerisinde aşağıdaki yer alan ana değişiklikler gerçekleştirilmiştir:[172]

- İdari ve finansal olarak tam anlamıyla bağımsız bir denetim ve gözetim otoritesi olarak BDDK'nın kurulması,
- Banka denetim ve gözetim yetkilerinin BDDK'ya devredilmesi,
- Banka kuruluşu için gereken şartların ağırlaştırılması,

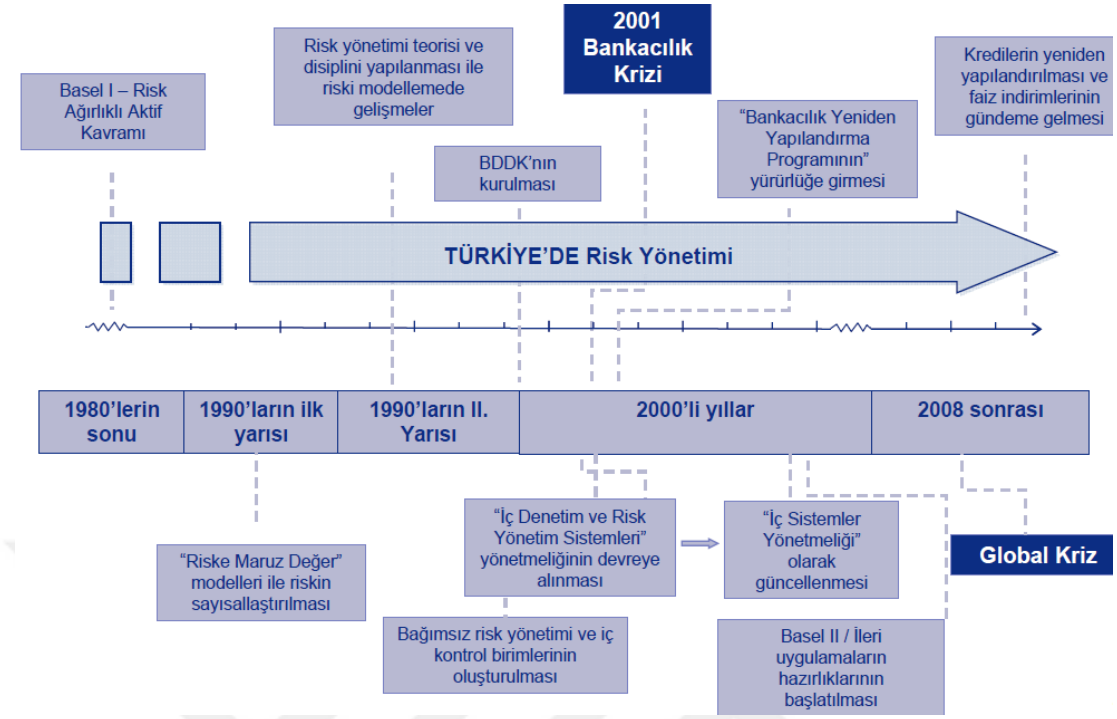
[172] Evren BOLGÜN ve Barış AKÇAY**, "Sermaye Piyasası ve Reel Sektör Uygulamaları"**, Scala Yayıncılık, 3. Baskı, İstanbul, 2009, s.124.

- Bankaların uygun bir iç denetim ve risk yönetim sistemine sahip olmalarının zorunlu hale getirilmesi,
- Kredi tanımlamalarında büyük kredi tanımına yer verilmesi ve kredi limiti kavramlarının oluşturulması,

4491 sayılı kanun 5411 sayılı Bankacılık Kanunun 01 Kasım 2005 tarihinde yürürlüğe girmesiyle birlikte geçerliliğini yitirmiştir. 5411 sayılı kanunun en önemli maddesi 29. Madde olup, söz konusu madde kapsamında bankaların karşılaştıkları riskleri izlemesi ve kontrolünün sağlanması görevi üst düzey yöneticilere, yönetim kuruluna ve çalışanlara verilmiştir. Bu sorumluluğun yerine getirilmesi amacıyla üst düzey yöneticileri, yönetim kurulunu ve çalışanları tam anlamıyla kapsamına dahil eden etkili bir iç kontrol sisteminin kurulmasından ve banka bünyesinde uygulanmasından sorumludur. İlgili kanun içerisinde 30. Madde kapsamında, "Bankalar, iç kontrol sistemi kapsamında, faaliyetlerinin mevzuata, iç düzenlemelerine ve bankacılık teamüllerine uygun olarak yürütülmesini, muhasebe ve raporlama sisteminin bütünlüğünü, güvenilirliğini ve bilgilerin zamanında elde edilebilirliğini her seviyedeki personeli tarafından uyulacak ve uygulanacak sürekli kontrol faaliyetleri ile sağlamak, görevlerin fonksiyonel ayrımlarını, yetki ve sorumlulukların paylaşımını, fon ödemelerini, banka işlemlerinin mutabakatını, varlıkların korunmasını ve yükümlülüklerin kontrol altında tutulmasını temin etmek, maruz kalınan her türlü riskin tanınması, değerlendirilmesi ve yönetimi için gerekli alt yapıyı hazırlamak ve yeterli iletişim ağını oluşturmak zorunda olduğu belirtilmiştir.[173]

Türkiye'deki bankacılık sektöründe oluşturulan kanunlara istinaden bankacılık sektöründeki risk yönetiminin gelişimi ve değişimi aşağıdaki gibidir:

[173] Nursu AYKUT, " Türk Bankacılık Sektörünün İç Kontrol Sistemi ve Risk Yönetimi Açısından Değerlendirilmesi ve Bu Bağlamda Basel II Kriterlerinin Sektöre Etkileri", **Dönem Projesi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2011, s.50.



Şekil 18: Türkiye Bankacılık Sektöründe Risk Yönetimi

Kaynak: KPMG Türkiye Finansal Danışmanlık Hizmetleri, "Türkiye'de ve Dünyada Bankacılık Sektörü Risk Yönetimi Uygulamaları ve Düzenlemeleri", 17 Aralık 2009, http://www.tbb.org.tr/Dosyalar/Konferans_Sunumlari/RiskYonetimi17.12.2009.zip, (13.12.2015), s.4.

2001 yılı içerisinde yaşanan bankacılık krizinin Türkiye bankacılık sektöründeki risk yönetimine etkileri aşağıdaki belirtildiği şekilde oluşmuştur:[174]

- "İç Denetim ve Risk Yönetim Sistemleri" yönetmeliği yürürlüğe girmiştir. Söz konusu yönetmelik 08.02.2001 tarihinde yayınlanmakla birlikte, 01.11.2006 tarihinde "İç Sistemler Yönetmeliği" olarak güncellenmiştir.
- "Bankacılık Yeniden Yapılandırma Programı" yürürlüğe girmiştir.
- Yürürlüğe giren yönetmelik ve mevzuatlarla birlikte bankalar bünyesinde bağımsız risk yönetimi, iç kontrol ve iç denetim bölümleri oluşturulmuştur.
- Yönetim kurulu risk yönetimi strateji ve politikalarının belirlenmesinden, iç sistemlerin kurulmasından ve etkinliğinin izlenmesinden nihai sorumlu hale gelmiştir.

[174] BİLGE, a.g.e, s.98.

- Denetim komitesinin yönetim kurulu adına iç sistemlerin etkinliğini izlemesi ve sonuçları yönetim kurulu ile paylaşması ana sorumluluğu haline gelmiştir.

BDDK tarafından 2012 yılında yayınlanan "Bankaların İç Sistemleri Hakkındaki Yönetmelik" içerisinde banka bünyesinde yürütülen risk yönetim sisteminin amacı tanımlanmıştır. Bu kapsamda risk yönetim sisteminin amacı; bankanın gelecekte tahsil edeceği nakit akışlarının ihtiva ettiği risk-getiri yapısını, buna bağlı olarak faaliyetlerin niteliğini ve düzeyini izlemeye, kontrol altında tutmaya ve gerektiğinde değiştirmeye yönelik olarak belirlenen politikalar, uygulama usulleri ve limitler vasıtasıyla, maruz kalınan risklerin konsolide ve konsolide olmayan bazda tanımlanmasını, ölçülmesini, raporlanmasını, izlenmesini, kontrol edilmesini ve risk profilleriyle uyumlu içsel sermaye gereksiniminin belirlenmesini sağlamak olarak ifade edilmiştir.[175]

2.7.2 Basel Kriterlerine Göre Risk Yönetimi

Banka denetiminde, bankaların bilançolarının zaman içinde gerçekleştirilen faaliyetlere bağlı olarak bilanço kalitesindeki değişiklikler ve yasal otorite tarafından belirlenmiş olan sermaye gereksinimleri ile uyumlu olup olmadığına odaklanılmıştır. Banka sermaye yapısının ve büyüklüğünün ölçülebilmesi; günümüz dünyasında finansal yeniliklerin artmasına bağlı olarak, finansal kurumlara ve yatırımcılara kısa sürede yüksek derecede kazanç sağlayacak yeni pazarların ve enstrümanların oluşması ile birlikte zor bir durum haline gelmiştir.[176]

1974 dönemi içerisinde uluslararası bankacılık ve finansal piyasalarda yaşanan dalgalanmalara bağlı olarak G10 ülkelerinin merkez bankası başkanlarının liderliğinde, bankacılık sektöründe gerçekleştirilecek olan denetim çalışmalarının kapsamını ve kalite

---

[175] Seyhan Çil KOÇYİĞİT ve Aysel DEMİR, "Türk Bankacılık Sektöründe Kredi Riski ve Yönetimine İlişkin Bir Uygulama: Türkiye Garanti Bankası Örneği", **İşletme Araştırmaları Dergisi**, Sayı:309, Temmuz 2012, s.226.

[176] Mahmut YARDIMCIOĞLU ve H. Gökçe DEMİREL, "Risk Yönetiminde Kriz Sonrası Yeni Finansal Mimariye Yönelik Bir Adım: Basel III", **Mali Çözüm Dergisi**, Sayı:125, Kasım-Aralık 2010, s.64.

standartlarının oluşturulması amacıyla Bankacılık Düzenleme ve Denetleme Uygulama Komitesi kurulmuştur. Komite;[177]

- Ulusal denetim sistemleri ile ilgili olarak bilgi paylaşımının yaygınlaştırılmasına,
- Uluslararası düzeyde uygulanabilir nitelikte olan denetim teknik, metot ve uygulamalarının etkililiğinin artırılmasına,
- İhtiyaç duyulan çalışma alanlarında minimum seviyede olacak şekilde denetim kriterlerinin oluşturulmasına yönelik çalışmalar yapmaktadır.

Dünya finans piyasalarında ve gelişmiş ülkelerde ortaya çıkan ekonomik krizler, bankacılık sektöründe faaliyet gösteren bankaların sermaye yapılarının ve yeterliliğinin öneminin artmasına neden olmuştur. Sermaye yeterliliği, bankaların sahip oldukları mali sorumluluklarını yerine getirmek ve bu sorumluluğu tam, doğru ve zamanında yerine getirebilmek amacıyla karşılaşabileceği muhtemel kayıplardan kaçınmak hedefiyle banka bünyesinde bulundurmaları gereken sermaye düzeyini ifade eder. Sermaye yeterliliği kavramına ait düzenleme, ilk olarak 1988 yılında Basel Bankacılık ve Denetim Komitesi tarafından oluşturulan Basel I düzenlemesi ile gerçekleştirilmiştir. Gerçekleştirilen ilk düzenlemenin riske karşı olan hassasiyetin düşük olması, sermaye yeterliliği ile ilgili olarak yeni bir düzenlemenin oluşturulmasına neden olmuştur. Bu nedenle 2004 yılı içerisinde "Yeni Basel Sermaye Yeterliliği Uzlaşısı - Basel 2" düzenlemesi oluşturulmuştur. Basel I düzenlemeleri uluslararası bankacılık sektöründe 1988 yılında uygulanmaya başlanmıştır. Basel I düzenlemeleri, Türk Bankacılık sektöründe 2007 yılında uygulamaya başlanmıştır.[178]

Basel I düzenlemeleri içerisinde kredi ve piyasa riski tanımlamaları yapılmıştır. Yapılan tanımlamalara istinaden söz konusu bu risklerin ölçülmesi ve takip edilmesi

---

[177] Turan YAY, Gülsün GÜRKAN YAY ve Ensar YILMAZ, "Finansal Krizler, Finansal Regülasyon ve Türkiye", **İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Sayı:30, Mart 2004, s.107.

[178] Sezai DUMANOĞLU ve Nuray ERGÜL, " Basel 2'nin KOBİ'ler Üzerindeki Muhtemel Etkileri", **Muhasebe ve Finansman Öğretim Üyeleri Bilim ve Araştırma Derneği Muhasebe ve Finansman Dergisi**, Sayı:43, Temmuz 2009, s.112.

öngörülmüştür. Yapılan düzenleme kapsamında, bankaların karşılaştığı kredi riski ve piyasa riskini ölçmede kullanılan metotların sorgulanmasına neden olmuştur. Yapılan sorgulama neticesinde; bankaların kullanmış oldukları yöntemlerle risk seviyelerini belirlemede ve ölçmede yeterli olmadığı, fiyat dalgalanmalarına ait sonuçları yeterince analiz etmediği, bankaların portföy oluşturma davranışlarının farklılık gösterdiği görülmüştür. Yapılan bu tespitler neticesinde; oluşturulan Basel I standardı yeniden değerlendirilerek kapsamının genişletilmesine kara verilmiştir. Ayrıca standart kapsamda yapılan risk ölçümlerinin daha hassas risk ölçüm ve yönetim metotlarına yer verebilecek şekilde yapılandırılması konusu değerlendirilmiştir.[179]

Basel I'in temel amacı; uluslararası bankacılık sisteminin istikrarını, emniyetini ve güvenirliğini korumak, bankaların risk kültürünü oluşturmak, yöneticilerin ve banka sahiplerinin bakış açılarını yeni düzenlemelere uyumlu olarak genişletmek, teknolojik yatırımları tamamlamak, personeli eğitmek ve farklı ülkelerdeki uygulamalarla yeknesaklık sağlamak, uluslararası bankalar arasında rekabet eşitsizliğini azaltmak olarak belirlenmiştir.[180]

Basel komitesi tarafından 1999 yılında oluşturulan 'Principles for the Management of Credit Risk' adlı doküman içerisinde kredi risk yönetimi sürecinin aşamalarına yer verilmiştir. Bu aşamalar; [181]

- Kredi riskiyle ilgili ilişkili olan çevresel ortamının oluşturulması,
- Kredi verme işlemlerine ait yürütülen faaliyetlerin bir bütün içerisinde etkili bir şekilde uygulanması,

---

179 Mahmut YARDIMCIOĞLU ve Murat BAY, "Türkiye'de Basel II'nin Kobilere Uygulanma Sorunları ve 2009 Yılı Bankacılık Sektörü Analizi", **Mali Çözüm Dergisi**, Sayı:101, Eylül-Ekim 2010, s.33.

180 Mikail EROL, "Basel I ve Basel II Uzlaşısının Bankalar Tarafından İşletmelere Verilen Kredilerde Risk Yönetimi Aracı Olarak Kullanılması", **Muhasebe ve Finansman Öğretim Üyeleri Bilim ve Araştırma Derneği Muhasebe ve Finansman Dergisi**, Sayı:36, Ekim 2007, s.156.

181 Basel COMMITTEE,"Principles for the Management of Credit Risk", 1999, http://www.bis.org/publ/bcbs75.pdf , (05.06.2012), s.1.

- Kredi riskinin tanımlanması, yönetimi, ölçümü ve izleme faaliyetlerinin devamlılığının sağlanması,
- Kredi riski ile ilgili olan kontrol yapısının içsel ve dışsal durumlar değerlendirilerek yeterli seviyede sağlanmasıdır.

Basel komitesi tarafından oluşturulan doküman içerisinde **kredi risk yönetimine ait temel unsurlar** aşağıdaki şekilde belirtilmiştir:

- Üst yönetim tarafından onaylanmış kredi risk stratejileri ve politikaları,
- Kredi risk yönetiminin organizasyonel yapısı,

Basel I düzenlemesi, düzenlemenin yapıldığı tarihteki sermaye hareketlerinin aynı seviyede kalmaması ve sermaye hareketlerine ait hacim ve adet sayısının artması, bankaların oluşturmuş olduğu kredi portföy yapılarının performanslarının beklenen seviyede olmaması ve buna bağlı olarak sermaye yeterliliği karşılama ihtiyaçlarının oluşması, kullanılan finansal enstrümanların farklılaşması nedeniyle revize edilmiştir. Bu nedenlerden dolayı; komite tarafından gerçekleştirilen revizeler kapsamında birlikte Haziran 2004 tarihi itibariyle Basel II sermaye yeterliliği düzenlemesi oluşturulmuştur.[182]

Basel I kapsamında eksik kalınan ve/veya eleştiri konusu olan alanlar:[183]

- Kredi riskinin ayrıştırılmasının sınırlı olmasına bağlı olarak risk duyarlılığının düşük olması: Düzenleme kapsamında 5 çeşit (0-10-20-50-100) risk ağırlığının kullanılmasının öngörülmesi,
- Kredi riskinin statik olarak ölçülmesi: Kredi riski ölçümünün değişen koşullara göre esneklik gösterememesi,
- Kredi vade bilgisinin risk değerlendirilmesinde dikkate alınmaması,

---

[182] Sadiye OKTAY ve Halim TEMEL, "Basel II Kriterleri Ekseninde Ticari Bankalarda Kredi Riski Yönetiminin Karşılaştırılmasına Yönelik Bir Saha Çalışması", **Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Dergisi**, Cilt:3, Sayı:6, 2007, s.165.

[183] Efsane CENGİZ, "Basel I-II-II Sermaye Uzlaşısı", **Yüksek Lisans Tezi**, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2013, s.13-14.

- Krediyi kullanan tarafın kredibilitesinin değerlendirilmemesi: Karşı tarafın kredi değerliliğine dikkat edilmemesidir.

Basel II düzenlemeleri kapsamında yukarıdaki belirtilen konular dışında, bankaların karşılaştıkları risklere, bankacılık faaliyetleri dışındaki yaşanan aksaklıkları, doğal afetler gibi nedenlerle ortaya çıkan risklere karşı **"operasyonel risk"** kavramını risk hesaplamalarına dahil edilmiştir.[184]

Basel II düzenlemesinde, kullandırılan kredilere bağlı olarak sermaye yükümlülüğünün belirlenmesinde kullanılacak olan kriterlerle ilgili olarak değişiklik yapılmıştır. Bu değişiklikler, işletmenin kendine ait derecelendirme notu ve çeşitli derecelendirme kuruluşları tarafından belirlenen derecelendirme notlarının sermaye yeterliliği hesaplamasında dikkate alınması ve kredi borçlusunun krediyi geri ödeme sorumluluğunu sağlayamaması durumunda bankanın zararını minimize etmeye yönelik olarak borçludan temin ettiği teminat çeşitlerinin hesaplama kapsamına dahil edilmesidir. Basel II'de uygulamasında sermaye yükümlülüğünün kredilerle ilişkili olan hesaplama kısmında 3 çeşit yaklaşım kullanımına yer verilmiştir. Bu yaklaşımlar, basitleştirilmiş standart yaklaşım, standart yaklaşım ve içsel derecelendirme modellerini dikkate alan yaklaşımlardır.[185] Basel II aşağıdaki belirtilen ihtiyaçları karşılamak amacıyla oluşturulmuştur:[186]

- Verimli ve etkili risk yönetimi ve piyasa disiplini geliştirmek,
- Sermaye yeterliliği ölçümlerinin etkinliğini ve efektifliğini artırmak,
- Etkili ve sağlam bir yapıya sahip olan bankacılık sisteminin oluşturulmasını sağlanmak,
- Finansal yapı içerisindeki istikrara katkıda bulunmayı sağlamaktır.

Basel II standardı içerisinde kredi kullandırılacak olan işletmelere ait risk ölçümü ve değerlendirmesi yapılırken işletmenin risk seviyesinin (faaliyet-işletme riski)

---

184 İlhan ÇİFTÇİ, "Basel II Çerçevesinde Operasyonel Risk İçin Sermaye Ayarlaması", **Yüksek Lisans Tezi**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2007, s.20.

185 DUMANOĞLU ve ERGÜL, a.g.m., ss.115.

186 EROL, a.g.m., ss.157.

ve kredi işlemine ait risk seviyesinin dikkate alınmasını belirtmiştir. Standart kapsamında işletme risk seviyesinin iki farklı kriter dikkate alınarak değerlendirilmesi gerektiği belirtilmiştir. Bunlardan birincisi, işletmenin finansal verilerinin değerlendirilmesi, diğeri ise işletmenin faaliyet riskinin değerlendirilip, ölçüldüğü işletmeye ait niteliksel (örn.yönetim-organizasyon yapısı, pazar payı, ürün-hizmet gelişimi vb.) özelliklerdir. Kredi riskinin değerlendirilmesinde; işletme sınıfı (çeşidi), kredi vade süresi, kredi için verilen teminat çeşidi ve miktarı, işletmenin mali yapısı ve durumu, işletmeye ait istihbarat geçmişi ve geçmiş yükümlülüklerini yerine getirme durumu değerlendirilir.[187]

Basel II standardı içerisinde Basel I uygulamasından farklı olarak; bankanın karşılaşabileceği bütün risk çeşitlerinin yönetilmesi ile ilgili olarak banka yönetim kurulu tarafından belirlenmiş bir risk stratejisinin oluşturulması gerektiği vurgulanmıştır.[188]

Basel II standardı kapsamında yer alan sermaye yeterliliği, yaşanan küresel krizle birlikte bankacılık sektöründe artan banka iflasları, denetim ve gözetim işlemlerinin sorgulanmasına neden olmuştur. Finansal piyasalarda gerçekleştirilen düzenlemeler ve buna bağlı olarak yatırımcıların kar etme isteklerindeki artış, finansal piyasalardaki risk iştahının artmasına neden olmuştur. Bu durum, sektör içerisinde faaliyet gösteren bankaların gözetim ve denetim faaliyetlerine ait periyot süresinin azalmasına, sıklığının artmasına neden olmuştur. Bu nedenle; gözetim ve denetim faaliyetine ait yeni tedbirlerin alınması gereği ortaya çıkmıştır. Basel Komitesi tarafından öngörülen ve oluşturulan yeni standartlar, 27 ülkenin merkez bankaları ve bankacılık düzenleme kurumları tarafından gerçekleştirilen çalışmalar ile 12 Eylül 2010 tarihinde Basel III Düzenlemeleri oluşturulmuştur.[189]

---

[187] A. Aslan ŞENDOĞDU, "Basel II Kriterlerinin Dünü Bugünü ve Gelecek İçin Bir Üst Sürümüne Olan İhtiyacın Kaçınılmazlığı", **Bankacılık ve Sigortacılık Araştırmaları Dergisi**, Cilt:1, Sayı:2, Haziran 2010, ss.7.

[188] OKTAY ve TEMEL, a.g.m., ss.169.

[189] İlhan ŞAHİN, " Küresel Finansal Kriz Esnasında Geliştirilen Bankacılık Düzenlemelerinden Basel III kriterlerinin Kapsamı ve Uygulama Süreci", **Muhasebe ve Finansman Dergisi**, Temmuz 2013, s.150.

Basel III kapsamında oluşturulan düzenleme değişikliklerine bağlı olarak belirlenen amaçlar;[190]

- Bankacılık sisteminin finansal ve/veya ekonomik değişikliklere ve şoklara karşı sağlam temeller üzerinde güçlü ve dirençli durmasının arttırılması,
- Kurumsal yönetişim ve risk yönetimi uygulamalarının geliştirilmesi,
- Bankaların şeffaflığının ve kamuya bilgi verme özelliklerinin artırılması,
- Mikro bazda yapılan düzenlemelerle bireysel olarak bankaların dayanıklılığının artırılması,
- Makro bazda düzenlemelerle finansal sistemin şoklara karşı direncinin artırılması.

Basel standart ve düzenlemeleri ile birlikte bankacılık sektöründe uygulanacak olan risk yönetimi ile ilgili olarak önemli yenilikler ortaya çıkarmıştır. Bu yeniliklerin öncelikli olanı bankaların sermaye yeterlilik oranlarının yükseltilmesi ve işletmelere verilen kredilerle ilgili olarak derecelendirme faaliyetinin gerçekleştirilmesidir. 1.1.2014 itibariyle Basel III uygulaması içerisinde stres testi, sermaye yeterlilik oranları ve piyasa likidite riski kavramlarına yer verilmiş ve ilgili kavramların üzerinde yoğunlaşılmıştır. Basel düzenlemelerinin bankaların risk yönetimini güçlendirmeleri yönünde katkı sağladığı görülmektedir.

[190] Eymen GÜREL, Esra Burcu BULGURCU GÜREL ve Neslihan DEMİR, "Basel III Kriterleri", **Bankacılık ve Sigortacılık Araştırmaları Dergisi**, Cilt:1, Sayı:3-4, Ocak 2012, s.18.

3. BÖLÜM
BANKALARDA BİLGİ TEKNOLOJİLERİNE AİT BENİMSENEN KONTROL HEDEFLERİ

3.1 Bankacılık Sektöründe Bilgi Teknolojilerinin Kullanılması ve Önemi

İşletmelerin operasyonlarını gerçekleştirdikleri sektör içerisinde rakiplerine göre avantaj sağlayacak olan ürün, hizmet ve faaliyetlerinin gelişim göstermesinde bilgi teknolojilerinin ve sistemlerinin kullanılması, bilgi sistemlerine ait stratejik rolün bir fonksiyonu olarak ortaya çıkar. Bilgi sistemi ve teknolojileri işletmelerde stratejik olarak, rekabet üstünlüğü kazanmak, verimliliği ve performansı arttırmak, yönetim ve organizasyonda yeni yöntemler geliştirmek ve yeni iş alanları oluşturma amacıyla kullanılabilir.[191]

Bilgi sistemlerinin ve teknolojilerinin yukarıdaki belirtilen fayda ve avantajları değerlendirildiğinde; bilgi sistemlerinin ve teknolojilerinin bankacılık faaliyetlerinde kullanılması bankalar açısından önem arz eder.

Genel olarak bankanın gerçekleştirmiş olduğu bankacılık hizmetleri, geçtiğimiz dönemlerde müşterilerin bankacılık işlemlerini gerçekleştirmek için bankanın ilgili şubesine fiilen gitmesi ve gerçekleştirmek istediği hizmeti talep etmesi olarak anlaşılmaktaydı. Bu ilerleyen aşamalarda teknolojinin gelişmesine bağlı olarak bankamatik yardımıyla şube dışından bankacılık işlemlerinin yapılmasına olanak sağlamıştır. Banka müşterilerinin fiili olarak banka şubesine gelerek işlemlerini gerçekleştirmesi, gerek bankaya, gerekse bankanın müşterisine oldukça yüksek bir maliyet oluşturduğu görülmektedir. Zamanın günümüzde çok önemli bir olgu olarak karşımıza çıktığı bir dönemde, bankaların sunmuş olduğu bankacılık hizmetlerinin maliyeti büyük önem arz etmektedir. Bankaların teknolojik yapıları ve işlemleri kullanmasındaki artış miktarı, sektör uygulamalarında geniş bir kitleye ulaşmayı hedef olarak belirlemelerine olanak sağlamıştır. Bu nedenle bankalar, hangi müşteri grubunu

[191] Dilek DEMİRHAN, "İşletmelerde Stratejik Bilgi Sistemleri Yönetimi ve Rekabet Üstünlüğü Elde Edilmesindeki Rolü", **Ege Akademik Bakış Dergisi**, Cilt:2, Sayı: 2, Temmuz 2002, s.118.

hedeflendiğini ve müşteri grubunun beklentilerinin neler olduğunu iyi bir şekilde tanımlamalıdır. Günümüzde bu tanımlamalar yapılırken, işletme bünyesinde yapılacak olan tanımlamalara ait stratejiler oluşturulmaktadır. Oluşturulan stratejiler en verimli şekilde kullanılarak, bankanın kullanmış olduğu teknolojinin buna göre geliştirilmesi ve şekillendirilmesi gereklidir. Aksi takdirde belirlenen stratejinin hayata geçirilmesinde problemlerin ve sorunların oluşması kaçınılmazdır. Teknoloji araç ve gereçlerinin bankacılık sektöründe uygulanması ile birlikte geleneksel bankacılık anlayışı tanımlamaları geçerliliğini yitirmiştir. Bu durum; bankacılık sektörüne ait tanımlamaların değişmesine ve yeniden şekillenmesine neden olmuştur. Bu nedenle, bankalar tarafından teknolojik değişimler ve uygulamalar kullanırken, kullanım bilincinin kurum içerisinde oluşturulmasına önem göstermelidir. Çünkü bu teknolojilerin uygulanması, sadece kurum içerisinde yürütülen operasyon maliyetlerinin azaltılması ve rekabet avantajı sağlamak için değildir. Teknolojilerin uygulanması, bankacılık sektörüne ait stratejilerin ve kurum organizasyonlarının tamamen farklılaşmasına neden olmaktadır.

Bankacılık sektöründe müşterinin beklentisi, verilen hizmetin kaliteli ve miktar olarak fazla olmasıdır. Bankanın beklentisi ise müşteriye sunulan hizmetin az maliyetle sunulmasıdır. Müşteri ve banka beklentilerinin ortak noktada buluşması durumunda rekabet açısından kuruma avantaj sağlanarak rekabet üstünlüğünün ortaya çıkması sağlanır. Teknolojinin verimli bir şekilde kullanılması, kurumun gerçekleştirdiği faaliyetlerdeki operasyon maliyetlerinin, kalite ve hizmet sayısının artmasını sağlamaktadır. Bankalar tarafından teknolojide meydana gelen gelişmelerin yakından takip edilmesi, bankaların sundukları hizmet maliyetlerini azaltılmasına neden olmakla birlikte; sundukları hizmet çeşidinin ve sayısının daha geniş bir kitleye ulaşmasını sağlar.

Bankacılık sektöründe rekabetin artmasına bağlı olarak, teknolojinin bilinçli bir şekilde kullanılması durumunda, bu durumun hem banka bünyesinde hem de müşteri memnuniyeti açısından olumlu sonuçlar getireceği bir gerçektir. Bu nedenle bankalar, kullanmış olduğu teknoloji içerisinde bir takım köklü ve/veya köklü olmayan değişikliklere gitmektedir. Mevcut durumda başarılı bankanın tanımı; müşterisinin dilediği süre içerisinde, dilediği yerde ve biçimde ulaşılabilen ve yararlanabilen banka olarak tanımlanmaktadır. Bu tanımdan çıkarılacak sonuç, teknolojiyi uygulamalarını

müşteri işlemlerinde daha fazla ve geniş bir alanda kullanan ve müşteri beklentilerine ve tatminini ön planda tutan bankaların bu kritere daha yatkın olduğu görülmektedir.[192]

Yukarıdaki bölümlerde bankacılık sektörünün karşılaştığı risk türlerini ve bankacılık sektöründe yaşanan teknolojik gelişmelerin sonuçlarını değerlendirdikten sonra bankacılık sektöründe yaşanan teknolojik gelişmelerin takip edilebilmesi, kontrol edilebilmesi ve denetlenebilmesi açısından, bankalarda gerçekleştirilen bilgi teknolojileri denetimi ve COBIT denetim standartlarına değinilecektir.

3.2 Bilgi Teknolojileri Standartlarının Gelişimi

İşletme içerisinde yürütülen faaliyetlere ait iş süreçleri yaşanan teknolojik gelişmelere bağlı olarak süratli bir şekilde kabuk değiştirmekte ve teknolojik uygulamalardan faydalanmaktadır. İşletme içerisinde hayata geçirilen teknolojik gelişim ve değişimler, işletme faaliyetlerinin hızlı ve etkili olmasını sağlar. Teknolojinin hızla yayılması ve değişmesi, beraberinde avantajları ve dezavantajları da ortaya çıkarır. Bilgi teknolojileri kullanılarak manuel olarak gerçekleştirilen işlemlerin, otomatik hale getirilmesi, bu faaliyetlerin izlenmesini, kontrol altına alınmasını ve denetlenmesini zorlaştırmaktır.

İşletme bünyesinde bilgi teknolojilerinin ve sistemlerinin karmaşık bir yapı içerisinde oluşturulması, bilgi teknolojileri ile ilgili olarak risk çeşitleri üzerinde olumsuz sonuçlarının oluşmasına bağlı olarak, yeni risk çeşitlerinin ortaya çıkmasına neden olabilir. Organizasyon içerisinde yer alan veriler ve bu verileri oluşturan sistemler önemlidir. Ancak en fazla odaklanılması gereken kısım bu verileri oluşturan sistemler olmalıdır. Bu nedenle organizasyon içerisindeki faaliyetlerini, bilgi sistemleri ortamını kullanarak gerçekleştiren işletmelerin, denetim çalışmalarına istinaden temin edilen verilerin daha güvenilir ve anlamlı olabilmesi için bu verilerin oluşmasını sağlayan bilgi sistemi yapılarının ve bu yapı içerisinde kullanılan faaliyet ve uygulamaların sağlıklı ve güvenilir bir şekilde çalışması sağlanmalıdır.[193]

---

[192] Feride Bahar IŞIN, "Teknoloji Araçlarının Bankacılık Sektöründe Uygulanabilirliği ve Türkiye'deki Bu Doğrultudaki Bankacılık Uygulamalarının Değerlendirilmesi", **İktisadi ve İdari Bilimler Dergisi**, Cilt:20, Sayı:2, Eylül 2006, s.118.

[193] İzzet Gökhan ÖZBİLGİN, "Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar",

İşletmeler bilgi sistemlerine ait alt yapıları oluştururken öncelikli olarak süreç ve risk odaklı olarak sistemlerini oluşturmakta, oluşturulan sistemin diğer süreçlerle olan ilişkilerini mutlaka dikkate almalıdır. Günümüzde, işletmelerde yer alan bütün bölümlerin bilgi teknolojilerine bağlı olarak faaliyetlerini yürüttüğü bir dönemde, işletmelerin vizyon ve stratejisini artık bilgi teknolojileri standartları oluşturmaktadır. Bilgi teknolojileri standartlarının oluşumu bu alandaki ihtiyaçların ortaya çıkmasından ve bilgi teknolojilerinin dünden bugüne her süreçte daha çok kullanılmasına bağlı olarak oluşmuştur.

Bilgi teknolojileri standartlarının en kapsamlı olanı COBIT (Bilgi Teknolojileri ve ilgili teknolojiler için Kontrol Hedefleri) uygulamasının gelişimi incelendiğinde, COBIT uygulaması öncelikli olarak 1996 yılında bir denetim kontrol listesi olarak kullanılmaya başlanmıştır. ISACA (Information Systems Audit and Control Association Information Systems Audit and Control Association) ve ITGI (IT Governance Institute IT Governance Institute) tarafından COBIT çerçevesi, 1992 yılında oluşturulmuştur.[194]

İş süreçlerinin, bilginin yönetimi açısından 7 temel kriteri dikkate aldığı görülmektedir. Bunlar;

- Etkinlik
- Verimlilik
- Gizlilik
- Bütünlük
- Erişebilirlik
- Güvenirlik
- Düzenlemelere uyum kriterlerinden oluşmaktadır.

COBIT uygulamalarının ikinci uygulaması 1998 yılında ortaya çıkmıştır. İkinci versiyon içerisinde; denetim faaliyetinin, süreç tamamlandıktan sonra gerçekleştirilmesi

Sayıştay Dergisi, Sayı:49, Nisan-Haziran 2003, s.123.

194 Vildan UZUNAY, "COBIT (Control Objectives for Information and Related Technology)" 2007, http://kontrol.bumko.gov.tr/Eklenti/4045,cobitpdf.pdf?0, (18.01.2014), s.3.

nedeniyle, denetim faaliyetinden önce standartların ve yapılması gereken işlemlerin belirlenmesi amacıyla daha anlamlı bir "kontrol standart" haline dönüştürülmüştür.

Kontrol standardı içerisinde kontrol tanımı yapılmıştır. Kontrol tanımı; "öncelikli olarak istenmeyen bir durumun önlenmesini sağlamak eğer önleme faaliyeti gerçekleştirilemiyor ise; istenmeyen durumu tespit etmek veya istenilmeyen bir durumun gerçekleşmesi durumunda; gerçekleşen durumun zararını en aza indirmek için sürece vereceği zararı asgariye indirmek için durumu düzeltmek" olarak tanımlanmıştır. Uygulamanın ikinci versiyonu içerisindeki tanımlama incelendiğinde; COBIT kısaltması içerisinde yer alan "C" harfine karşılık gelen kelimenin, standart tanım içerisinde belirtilen anlamı karşıladığı görülmektedir. 1996 yılında yayınlanan ilk versiyon içerisinde bir denetim kontrol listesi olarak ortaya çıkan COBIT uygulaması, 1998 yılında yayınlanan versiyonuna "kontrol" tanımı dahil edilmiştir. 2000 yılına kadar kontrol odaklı bir yaklaşımı olması nedeniyle, COBIT uygulamalarının aslında 1996 – 2000 yılları arasında olgunlaştığı görülmektedir.[195]

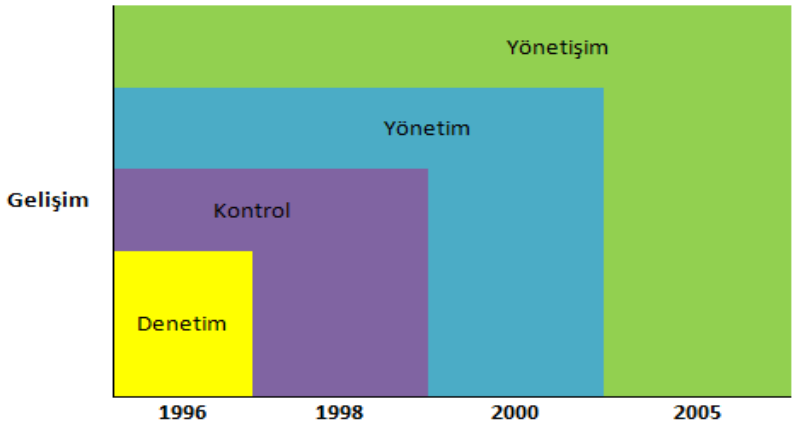
2000 yılı içerisinde oluşturulan COBIT yaklaşımında "bir süreç ile ilgili olarak kontrol faaliyetinin uygulanabiliyor olması, ilgili sürecin yönetilebiliyor olduğunu gösterir" şeklinde bir anlayış yer almaktadır. İlgili COBIT yaklaşımında söz konusu yönetim anlayışı dikkate alınarak, yönetim faaliyetinin en iyi bir şekilde nasıl gerçekleştirilebileceği ile ilgili olarak araştırmalar yapılmaya başlanmıştır. Yapılan çalışmalar kapsamında COBIT'in aynı zamanda bir yönetim çerçevesi olduğu ve buna bağlı olarak COBIT 3 versiyonu oluşturulmuştur. COBIT 3 uygulaması içerisinde, yönetim rehberi, ölçüm kriterleri, yönetsel özet, kontrol hedefleri, uygulama rehberi, denetim rehberi vb. yönetişim araçlarına yer verilmiştir.[196]

Kurumsal yönetim kavramı ve anlayışı işletmelerin içerisinde yer almaktadır. COBIT uygulaması işletmeler içerisinde yaygınlaşıp, gelişim devamlılığını arttırdığından; COBIT uygulaması 2005 yılında bilgi teknolojilerinin kurumsal yönetişim yöntemi olarak dönüşüme uğramıştır. 2007 yılında oluşturulan COBIT 4.0 ve 4.1

[195] Mehmet Cüneyt ÜVEY, "Orkestra Şefiniz: COBIT", **CIO Club**, Mayıs 2009, s.55.

[196] ÜVEY, a.g.m., ss.56.

versiyonları ise, iş süreçleri ile bilgi teknolojileri süreçlerini bir bütün olarak değerlendirilmesini sağlamıştır. Özellikle "stratejik uyum, katma değer yaratmak, kaynakların etkin ve verimli yönetimi, risklerin yönetimi ve performansın ölçümlenebilmesi"ne ait alanların uygulanmasına katkı sağlamıştır.[197]



Şekil 19: COBIT Standartlarının Gelişimi
Kaynak: Mehmet Cüneyt ÜVEY, "Orkestra Şefiniz: COBIT", **CIO Club**, Mayıs 2009, s.55.

COBIT yapısı bakımından incelendiğinde; **4 temel faaliyet** alanı altında gruplanmış olan **34 adet alt süreçten** oluşmaktadır. Her bir süreç ile yukarıda belirtilen **7 adet bilgi standardı** ve 4 adet bilgi teknolojileri kaynağı (Uygulamalar, Bilgiler, Altyapı ve İnsan Kaynakları) arasındaki bağlantılara yer verilmiştir. COBIT standartlarında; bilgi teknolojileri ile ilgili olan her bir sürecin, bilgi teknolojileri yönetişiminin sağlanabilmesi amacıyla hangi yönetsel boyuta hizmet verdiğinin bağlantısı net olarak tanımlanmış ve bağlantısı kurulmuştur. Ayrıca COBIT uygulaması içerisinde yer alan bölümlerin hangi bölümünün hangi süreçlere girdi sağladığı ve hangi süreçlerin çıktılarından yararlandığı da açıkça ortaya koyulmuş olup, süreçlerin birbirleri ile olan ilişkileri tanımlanmıştır. COBIT uygulamaları, diğer standartların ve uygulamaların tamamlayıcısı olarak ortaya çıkmıştır. Diğer detaylandırılmış olan uygulama ve standartlar, ITIL, ISO 27001 ve 27001 ve PMBOK (The Project

[197] ÜVEY, a.g.m., ss.56.

Management Body of Knowledge) spesifik alanları kapsamakla birlikte COBIT uygulaması ile eşleştirilmiştir. Standartlar, iş süreçlerine ait spesifik ihtiyaçlara fayda sağlaması açısından uygulanmalıdır.

ITIL uygulaması, 1980'li yılların sonunda Birleşmiş Krallık Ticaret Ofisi tarafından geliştirilen bir uygulamadır. ITIL, Birleşik Krallık hükümetinde bilgi işlem servis yönetimini iyileştirmek amacıyla hazırlanmıştır. ITIL (Information Technology Infrastructure Library-Bilgi İşlem Altyapı Kütüphanesi) uygulaması, işletme bünyesindeki operasyonel bilgi işlem faaliyetlerinin tam, doğru ve beklenen kalite kapsamında gerçekleştirilmesi için oluşturulmuş ve geliştirilmiş uluslararası hizmet yönetimi metodolojisidir. ITIL, bilgi teknolojileri uygulama standartları açısından en uygun standart olarak gösterilmektedir. ITIL uygulama standartlarının referans olarak gösterilmesinin nedeni; bilgi teknolojileri hizmet yönetimi konusundaki uygulama verimliliğidir. ITIL, kaliteli bilgi teknolojileri hizmet yönetimi ve sunumunun kaliteli bir şekilde gerçekleştirilmesini sağlar. Standart kapsamında işletmelere teknolojik altyapı oluşturmak için yol gösterir. Standardın amacı, bilgi teknolojileri organizasyonlarının kendi ana iş süreçlerine özgü uyarlamalarla, bilgi teknolojileri yönetim ve işletimine yönelik süreçleri ve kontrolleri oluşturan bir metodoloji ortaya koymaktır.[198] ITIL standardı kapsamında bilgi işlem süreçlerine ait tanımlamalar ve dokümantasyon işlemleri kalite sistemlerinin belirlediği şekilde yapılır.

COBIT'in yönetime yönelik yaklaşımı ITIL uygulamalarına göre farklılık göstermektedir. Uygulamalar arasında farklılıklar bulunmasına rağmen; her iki uygulamanın da birbirini tamamladığı alanlar bulunmaktadır. COBIT'e ait son uygulama versiyonu ITIL uygulaması ile bağlantılı hale gelmiştir. ITIL uygulaması daha çok bilgi teknolojileri içerisinde yer alan faaliyetlerle ilgilenir. COBIT uygulaması ITIL standartlarında yer alan süreçleri kapsamakla birlikte, iş gereksinimlerinin ne şekilde karşılanacağını hedef olarak belirler. İşletmelerde yürütülen faaliyetlere bağlı olarak oluşan iş ihtiyaçlarının bilgi teknolojileri ile örtüşmesi, işletme masraflarının tam olarak ölçülmesini ve hizmet seviyeleri ile performans hedeflerinin oluşmasını sağlayabilir.

[198] Jimmy HESCHI, " Mapping ITIL v3 to COBIT", **COBIT Focus**, Ocak 2008, s.14.

COBIT ve ITIL uygulamaları iş ihtiyaçlarının bilgi teknolojileri işlemleri ile örtüşmesini sağlamaktadır.[199]

İşletme içerisinde üretilen ve/veya işletmenin faaliyetlerini yürütebilmesi için kullanmış olduğu bilgi, işletmenin faaliyetleri ve işletmenin devamı için önemlidir. ISO 27001/2 standardı uygulaması; değerli bilgi varlıklarının yönetilmesini ve korunmasını sağlar.

ISO 27001/2 standardı içerisinde bilgi güvenliği yönetimi sistemi gereksinimleri tanımlanmış olup, uluslararası denetlenebilir nitelikte bir standart olarak kabul edilmiştir. ISO 27001/2 standardının amacı, işletme bünyesindeki risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürlerinin hazırlaması ve uygulamada bu bilgilere ait kayıtların tutulmasıdır. Bu amacın gerçekleştirilebilmesi için işletme tarafından genel işletme bilgi güvenliği politikası oluşturmalı, işletme bünyesinde duyurulmalı ve işletme çalışanlarının bilgi güvenliği ve tehditleri ile ilgili olarak bilgilendirmesini sağlamalıdır. İşletme içerisinde oluşturulan kontrollere ait kontrol hedeflerinin ölçülmesi ve kontrollerin işletme hedef ve amaçlarına olan uygunluğunun ve performansının izlenmesi ve takip edilmesi gereklidir. Bu durum yönetimin aktif desteği ve çalışan personelin katılımı ile sağlanabilir.[200]

ISO 27001/2 standardı bir güvenlik standardı olup, diğer standartlardan farklıdır. Aşağıdaki tablo içerisinde standartlar arasındaki farklar belirtilmiştir:[201]

---

199 HESCHI, a.g.m., ss.15.

200 Fulya DOĞANTİMUR, "ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği", Maliye Bakanlığı Strateji Geliştirme Başkanlığı **Mesleki Yeterlilik Tez**i, 2009, s.8-9.

201 Anjar PRIANDOYO, "Comparison between COBIT, ITIL and ISO 27001", 2012, http://www.securityprocedure.com/comparison-between-cobit-itil-and-iso-27001, (02.06.2013), s.2.

Tablo 2: Bilgi Teknolojileri Standartlarının Karşılaştırılması

İş Süreci	COBIT	ITIL	ISO 27001/2
Fonksiyon	Bilgi teknolojileri süreçlerinin eşleştirilmesi	Yönetim düzeyinde bilgi teknolojilerinin eşleştirilmesi	Bilgi güvenliği uygulaması
İş alanı	4 temel faaliyet alanı ve 34 Süreç	9 temel faaliyet alanı	10 Süreç
Oluşturan Kurum	ISACA	OGC	ISO Kurulu
Uygulama	Bilgi Sistemleri Denetimi	Servis Düzeyinde Yönetim	Bilgi güvenliği standartlarına uyum
Danışman	Muhasebe firmaları, Bilgi Teknolojileri Danışmanlığı firmaları	Bilgi Teknolojileri Danışmanlığı firmaları	Bilgi Teknolojileri Danışmanlığı firmaları, Bilgi Güvenliği firmaları, Network Danışmanlığı

Kaynak: Anjar PRIANDOYO, "Comparison between COBIT, ITIL and ISO 27001", 2012, http://www.securityprocedure.com/comparison-between-cobit-itil-and-iso-27001, (02.06.2013), s.2.

Yukarıdaki tabloda yer alan karşılaştırma incelendiğinde; hangi standardın öncelikli olarak uygulanması ile ilgili olarak kesin bir durum bulunmamakla birlikte hangi standardın uygulanması gerektiği, işletmelerin ihtiyaçlarına göre farklılık göstermektedir. Çoğu işletme ilk uygulama olarak COBIT standartlarını organizasyon yapısında uygulamaktadır. Bunun en önemli nedeni, COBIT standardının bütün bilgi sistemini kapsamasından kaynaklanmaktadır. COBIT uygulamasından sonra işletmelerin tercihi ITIL veya ISO 27001/2 uygulamalarıdır.

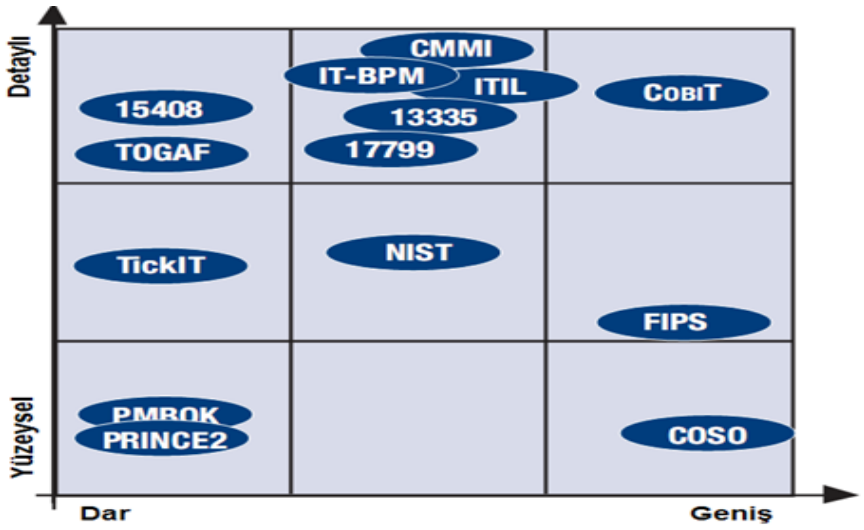
COBIT, ITIL veya ISO 27001/2 uygulamalarından hangisinin uygulanacağı ağırlıklı olarak işletmenin bütçesine bağlı olarak değişmektedir. ITIL veya ISO 27001/2 uygulamaları için bilgi teknolojileri bölümüne ait belirlenmiş olan bütçeden kaynak oluşturulmakla birlikte, COBIT uygulamaları genel olarak iç denetim bütçesinden kaynak sağlanarak oluşturulmaktadır. Bu durum işletme yönetiminin politikasına göre değişiklik göstermektedir. Hangi uygulamanın öncelikli olarak kullanılacağı işletme yönetiminin politikasına bağlı olarak değişkenlik gösterebilir.

Uygulama açısından standartlar değerlendirildiğinde, ITIL standardının en kolay uygulanabilir standart olduğu ortaya çıkmaktadır. Çünkü ITIL standardı, kısmen uygulanabilir olup, performansa etkisi olmadığından performans bağımsız olarak değerlendirilmektedir. Örneğin, işletmenin bilgi teknolojileri bölümüne ayırmış olduğu sınırlı bütçe nedeniyle; ITIL standartlarının bir bölümünün belirlenen zaman dilimi içerisinde bir kısmının; diğer kısımlarının ise başka zaman diliminde uygulanması sağlanabilir. ITIL uygulamasının yanı sıra; COBIT ve ISO 27001/2 standartlarının kısmen uygulanması oldukça zordur. İlgili standartlara ait uygulamaların kısmen olarak uygulanmasından önce işletme faaliyetlerinin genel olarak değerlendirilmesi ve incelenmesi gereklidir.

İşletme bünyesinde diğer standartların uygulanmaması, COBIT uygulamalarının daha fazla uygulanmasının amacı, işletmelerde bilişim teknolojileri, işin kendisi ve denetim birimleri arasındaki işbirliği geliştirmektedir. COBIT uygulamalarının en iyi şekilde uygulanması, işletme bünyesindeki bilişim teknolojileri bölümlerinin katma değerlerini en iyi şekilde sunma imkânı sağlar.

Şekil 20: Bilgi Teknolojileri Standartlarının Bileşimi

Aşağıdaki yer alan şekil içerisinde standartların kapsamlarına göre sınıflandırması yer almakla birlikte aşağıdaki tabloda COBIT'in diğer standartlara göre kapsamının hangi seviyede olduğu gösterilmeye çalışılmıştır.



Şekil 21: Bilgi Teknolojileri Standartlarının Kapsam Seviyesi
Kaynak: Ahmet Türkay VARLI, "Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi- Mevzuat Çerçevesinde BDDK Perspektifi", 09 Kasım 2007, www.bddk.org.tr/WebSitesi/turkce/Raporlar/Sunumlar/4020TIDE_Sunum.pdf, (12.03.2010), s.44.

COBIT standardı ilk oluşturulurken; COSO kontrol modelini örnek almıştır. COBIT uygulaması bilgi teknolojilerine ait süreçleri ve kontrolleri dikkate alarak oluşturulmuş bir standarttır. COBIT standardı kapsamında oluşturulan model ile bütün bilgi teknolojileri süreçlerine kuşbakışı olarak üst taraftan bakılabilmektedir. İşletme bünyesinde oluşturulmuş olan iç denetim ve kontrol süreçlerine ait faaliyetler dokümante edilir ve üst yönetim tarafından onaylanır. Süreçlere ait dokümante edilen faaliyetlerde, yapılan işlemlere ait performans ölçüm kriterleri, sürece ait girdi ve çıktı verileri tespit edilir. Dokümante edilmiş olan süreç kapsamında, gerçekleştirilen faaliyetlerle yazılan faaliyetlerin tutarlılığı ve sürekli iyileştirme gibi gereksinimler değerlendiriliyor ise; işletme bünyesinde genel ve kabul edilebilir bir sistem oluşturulduğundan söz edilebilir.

COBIT uygulamalarına ait iş süreçleri bilgi teknolojileri bölümlerinde uygulanmakta ve ilgili bölümün oluşturulan süreç içerisindeki konumu ve yeri belirlenmiştir. COBIT uygulamasındaki yer alan 34 adet uygulama her işletmeye uygulanabilir ve uyarlanabilen bir standart uygulama bütünü değildir. Ancak söz konusu uygulama standartlarının tüm süreçleri dikkate alabilmek için, büyük ve olgunlaşmış organizasyonlarda kullanılması etkinlik ve verimlilik sağlamaktadır. COBIT uygulamalarını gerçekleştirmek isteyen işletmeler, COBIT uygulamalarını gerçekleştirirken, faaliyetlerinde oluşabilecek olan kısıtlamaları ve aksamaları dikkate almalı, söz konusu kısıtlamaların ve aksaklıkların oluşmasına olanak sağlamamalıdır. Standart kapsamında yer alan uygulamaları gerçekleştirmek, zaman, emek ve maddi yeterliliğe dayanmaktadır.

3.3 Temel COBIT Bileşenleri ve Bileşenler Arasındaki Etkileşim

COBIT, sistematik bir yaklaşımdan yola çıkarak, işletme içerisindeki yönetsel faaliyetlere ait ihtiyaçlara ve beklentilere karşılık verecek şekilde oluşturulmuştur. COBIT iş hedeflerini bilgi işlem hedeflerine dönüştürerek, dönüştürülen hedefleri tamamlayabilmek için gerek duyulan ihtiyaçları belirleyen ve iş akışlarını toparlayan bir uygulamadır. Bilgi teknolojileri açısından COBIT, "Kontrol Hedefleri" anlamına (Control Objectives for IT and related Technologies) gelmektedir.

COBIT uygulamasının iskeleti, bilgi teknolojilerinin karşılaşmış olduğu riskleri, bu risklerin değerlendirilmesini, ortadan kaldırılmasına ilişkin kontrol faaliyetlerini ve belirlenmiş olan kontrollerin denetlenmesi ile ilgili olan faaliyet ve yöntemlerini ele alan bir yapıya sahiptir.[202]

[202] Eliza Natasa ARTİNYAN, "Cobit Çerçevesi", Deloitte Yayınları, 2007, http://www.denetimnet.net/UserFiles/Documents/Makaleler/BT%20Denetim/CobiT%20%C3%87er%C3%A7evesi.pdf, (24.06.2012), s.1.

Şekil 22: COBIT Bileşenleri
Kaynak: ISACA, "COBIT 4.1 Framework Control Objectives Management Guidelines Maturity Models", 2007, s.10.

COBIT ürünleri 3 ana seviyede organize edilmiş olup, aşağıda yer alan konuları desteklemektedir:[203]

• Üst düzey yönetim ve kurulunu

• İş ve bilgi teknolojileri yönetimini

• Yönetişim, güvence, kontrol ve güvenlik profesyonellerini

Belirtilen 3 ana seviyeye ait organizasyon bağlantısının kuvvetli olması, söz konusu ürünlerin işletme bünyesindeki koordinasyonunun etkin ve verimli bir şekilde yerine getirilmesine bağlı olarak uygulamanın işletme bünyesinde başarılı olmasına olanak sağlar.

İşletmeye ait bilgi teknolojilerine yönelik iç kontrol ortamının ve/veya çerçevesinin tesis edilmesi işletme yönetiminin sorumluluğundadır. Söz konusu ortamın

[203] ISACA, "COBIT 4.1 Framework Control Objectives Management Guidelines Maturity Models", 2007, s.7.

ve çerçevenin tesis edilmesi bilgi teknolojilerinin iş amaçlarına uygun olarak hizmet edilmesini sağlar. Bu nedenle; COBIT uygulaması ihtiyaca yönelik olarak aşağıdaki belirtilen faaliyetlere yardımcı olarak katkıda bulunmayı hedefler.[204]

- İş kollarına ait iş gereksinimlerine bağlı olan bilgi teknolojileri faaliyetlerini tespit ederek, söz konusu gereksinimler ile faaliyetler arasındaki bağlantının sağlanması ve korunması,

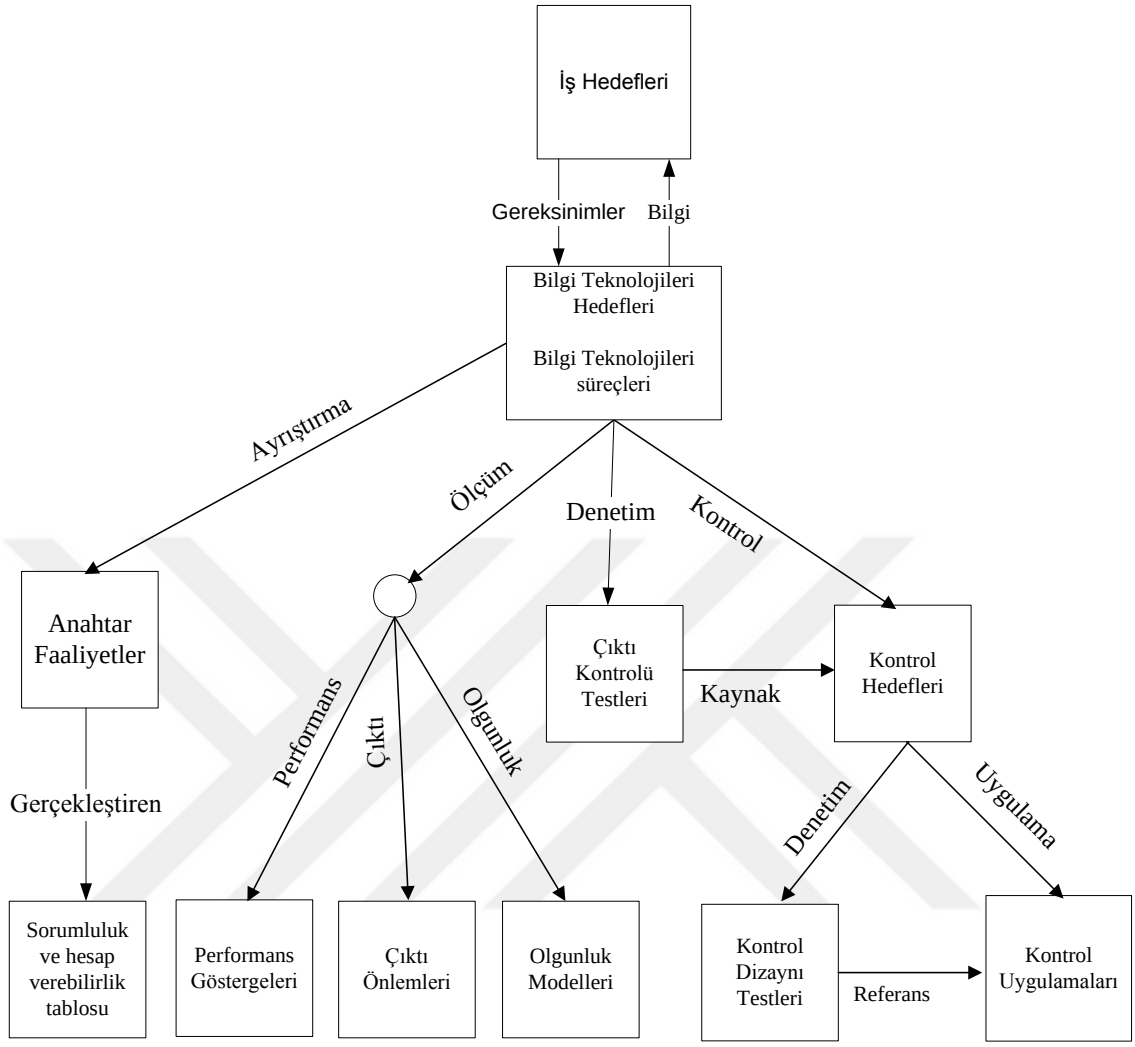
- İşletmeye ait bilgi teknolojileri faaliyetlerinin, genel kabul görmüş olan standartlara göre yönetilmesi ve/veya organize edilmesi,

- Bilgi teknolojilerine ait kaynak envanter listesinin oluşturulması, belirlenmesi ve işletme hedeflerine yönelik olarak yönetilmesi,

- İşletme yönetiminin kontrol hedeflerini bilgi teknolojileri faaliyetleri alanında ve kapsamında belirlemek,

COBIT uygulamasının bütün bileşenleri kendi aralarında bağlantılar oluşturarak, yönetişim, yönetim, kontrol ve güvence ihtiyaçlarına destek sağlar. COBIT bileşenleri arasındaki bağlantılar aşağıdaki şekilde gösterilmiştir:

[204] ISACA, a.g.e., s.6.



Şekil 23: COBIT Bileşenleri Arasındaki İlişki
Kaynak: ISACA, "COBIT 4.1 Framework Control Objectives Management Guidelines Maturity Models", 2007, s.8.

COBIT süreçlerinin yapısı iş odaklı olarak üst düzey bir yaklaşımdan hareket ile bir bütün olarak baştan sona bilgi teknolojileri süreçlerinin gözden geçirilmesini sağlar. COBIT uygulaması yöneticilerin; kontrol gereksinimleri, teknik konular ve iş risklerinin bağlantılarının kurulmasını sağlar. İşletme yöneticileri, kontrol seviyesindeki iletişim kurma faaliyetlerini COBIT uygulaması aracılığıyla yerine getirir. COBIT uygulaması; işletmelerdeki bilgi teknolojileri kontrollerinin, diğer işletmelerdeki en iyi kontrol uygulamalarını dikkate alarak gelişmesine katkı sağlar. COBIT uygulaması diğer birçok standart ve rehber ile bir bütün olarak ele alınmış ve günümüze kadar gelişimini sürdürerek işletmelere katkı sağlamıştır. COBIT uygulamasına ait yapı içerisinde bilgi

teknolojileri için en iyi uygulamalar düzenlenmiş olup, bilgi teknolojileri alanında yer alan risklerin, faydaların anlaşılmasına ve yönetilmesine yardımcı olur. COBIT uygulamasının işletmeye ait bilgi teknolojilerinde uygulanması aşağıdaki yer alan kazanımların oluşmasını sağlar:

- İşletmeye ait iş süreçleri dikkate alınarak, işletmenin ihtiyaçlarını sağlayacak olan iyi bir önceliklendirmenin yapılması,

- Bilgi teknolojileri süreçleri değerlendirilirken, işletme yönetimin bakış açısı öncelikli olarak dikkate alınarak, yönetim bilgilendirmesinin yönetim bakış açısına uygun ve anlaşılır bir biçimde yapılması,

- İş süreçleri dikkate alınarak, iş kolu bazında sorumluluk ve yetkilendirmenin açık bir şekilde yapılması,

- Bilgi teknolojilerine ait uygulanan iş süreçlerinin işletme dışındaki üçüncü taraflar ve düzenleyici kurumlar tarafından kolay bir şekilde anlaşılabilir olması,

- İşletme bünyesinde ortak bir dil oluşturularak, bütün paydaşlar arasında paylaşılabilir ve anlaşılabilir nitelikte olması,

- Bilgi teknolojileri kontrol ortamı kapsamında COSO gereksinimlerini yerine getirmesi,

İşletmenin faaliyetlerini yürütürken ihtiyaç duyduğu ve/veya kullandığı bilginin, önemli ölçüde dış ve iç etkenlerden etkilenmesi, işletmenin gelişimi açısından olumsuz durumların yaşanmasına neden olabilir. İşletme üst yönetimi tarafından bilgi teknolojileri operasyonlarına ait beklentilerin yükselmesi ve işletmenin rekabet avantajı sağlayabilmesi amacıyla bilgi teknolojilerinin kaldıraç gücü etkisinin yüksek seviyelerde olduğunu kabul eder. Üst yönetimin ihtiyacı olan bilgi, aşağıdaki özellikleri taşıması durumunda işletme bünyesindeki bütün organizasyonel yapı içerisinde kullanılır ve yönetilir. Bu özellikler;

- Bilgi; işletme hedeflerine ulaşmaya yakındır,

- Bilginin öğrenilmesi ve uyarlanması için esnek olması yeterlidir,
- Bilgi teknolojilerinin karşılaştığı risklerin asgari ve makul bir seviyede yönetir,
- Ortaya çıkan fırsatların ve fırsat olarak ortaya çıkabilecek olan durumları işaret eder.

Sektöründe başarılı olan işletmeler, kullandıkları bilgi teknolojileri risklerini ve faydalarını dikkate alarak bunlardan yararlanır. Bu işlemleri yaparken aşağıdaki konulara dikkat eder:

- İşletmenin belirlemiş olduğu iş stratejileri ile birlikte bilgi teknolojileri stratejilerini birlikte bir öncelik sırasına göre sıralandırılmasına,
- İşletmenin iç ve dış paydaşlarına, işletme tarafından karşılaşılan bilgi teknolojileri risklerinin aktarılması,
- İşletme bünyesinde bilgi teknolojileri stratejilerinin ve hedeflerinin basamak halinde organizasyon yapısı içerisinde en üst seviyeden en alt seviyeye kadar oluşturulması,
- İşletme tarafından yapılan bilgi teknolojileri yatırımlarından değer elde edilmesini sağlayacak mekanizmalarının oluşturulması ve söz konusu bu mekanizmaların etkinliğinin ve verimliliğinin periyodik olarak gözden geçirilmesi,
- Üst yönetim tarafından belirlenen strateji ve hedeflerin uygulanabilmesinin kolaylaştırılabilmesi amacıyla organizasyonel yapının niteliğinin ve niceliğinin göz önüne alınması,
- İşletmenin iç ve dış ortamındaki etkili ve efektif bir iletişim kanalının oluşturulması amacıyla dışarıdan sağlanan ve/veya içyapı içerisindeki bilgi akışları, iş süreçleri ve bilgi teknolojileri arasında yapısal iletişim yapısının kurulmasının sağlanması,

- Bilgi teknolojileri performansının periyodik olarak ölçümlenmesi ve gözden geçirilmesi,

COBIT uygulaması ile birlikte; işletmenin yönetişim ve kontrol yapısı, bilgiye ihtiyacı olan her bir iç ve dış paydaşların bilgi ihtiyacının daha etkin ve verimli bir şekilde karşılanmasını sağlar. Örneğin;

- İşletme içerisinde yer alan paydaşlar, yapılan bilgi teknolojileri yatırımlarının değer yaratmasını bekler. Bu nedenle; söz konusu paydaşlar;

  - Yatırım kararlarının verilmesinde rol oynar,

  - İşletme gereksinimlerinin belirlenmesini sağlayarak, işletmeye en uygun olan bilgi teknolojilerinin uygulanmasını ve uygulamaya bağlı olarak uygulamanın etkinliğinin ve verimliliğinin sağlanmasından sorumlu olur.

- İşletmenin organizasyonel yapı içerisinde bilgi teknolojileri servislerini sağlayan iç ve/veya üçüncü taraf olarak nitelendirilen dış paydaşlar:

  - Bilgi sistemleri organizasyonunun ve süreçlerinin oluşturulmasında ve yönetiminde rol alır,

  - İşletmenin sektörel ve/veya üst yönetimi tarafından belirlenen stratejisine ve/veya hedefine göre bilgi teknolojileri yapısına ait kapasitenin arttırılmasında rol oynar,

  - Bilgi teknolojileri alt yapısı içerisinde oluşturulan servislerin kullanılmasında rol alır.

- İşletme bünyesinde risk ve kontrol sorumluluğuna sahip olan paydaşlar tarafından;

  - Risk ve kontrol kavramlarına ait sorumluluklar güvenlik, gizlilik ve/veya risk sorumluluklarından oluşur,

  - Bilgi teknolojileri içerisinde oluşturulan uyum fonksiyonlarının yerine getirilmesi,

- İşletme için gerekli görülen güvence hizmetlerinin sağlanması,

Bilgi teknolojileri içerisinde yer alan yönetişim ve kontrol kavramları aşağıdaki belirtilen koşulları oluşturur:

- İş süreçleri ve bilgi teknolojileri hedeflerinin sıralanmasını sağlayarak, iş odaklanmasının oluşmasını sağlar.
- İşletme içerisindeki süreç oryantasyonun kurulmasını sağlayarak, kapsamın büyüklüğünün ve içeriğinin tanımlanmasını sağlar.

COBIT uygulaması 4 ana prensipten oluşmaktadır. Bunlar;

1) İş odaklı

2) Süreç odaklı

3) Kontrol tabanlı

4) Ölçüm odaklı

1) İş Odaklı:

COBIT uygulamalarının temelini iş odaklılık oluşturur. İş odaklılık olma kriteri, bilgi teknolojileri servisini sağlayan çalışanlar, kullanıcılar ve denetçiler için oluşturulan bir yapı olmamakla birlikte; yönetim ve süreç sahiplerine işlemlerini yürütürken uygulamaları gereken bir rehber olarak dizayn edilmiştir.

COBIT uygulamalarının iş odaklı olması; işletme hedeflerine ulaşabilmek için gerekli olan bilgiyi elde edebilmek için kullanacak olan bilgi kaynağını ve bilgi kaynağının temin edildiği bilgi teknolojileri süreçlerinin yapılandırılmasına olanak sağlar. Bilgi teknolojilerine ait süreçler yapılandırılırken; süreçlerin yönetilmesi ve kontrol edilmesine olanak sağlanır. Bu kapsamda kontrol edilen ve yönetilen bilgiler; COBIT uygulamalarının kalbini oluşturur. Bilgilerin kontrol edilmesi ve yönetilebilmesi işletme bünyesindeki iş gereksinimlerine ait önceliklendirmelerin yapılmasına katkı sağlar. COBIT uygulaması içerisinde bilginin 7 çeşit kriteri bulunur. Bu kriterler;

a) Etkililik: İşletme bünyesinde kullanılacak olan bilginin işletme içerisindeki iş süreçleri ile ilişkili ve uygun olması gereklidir. Bilginin zamanında doğru, tutarlı ve kullanılabilir bir şekilde iletilmesi, bilginin etkili olduğunu gösterir.

b) Verimlilik: İşletme kaynaklarının en uygun ve en ekonomik kanal ile temin edilmesi verimlilik olarak tanımlanmaktadır.

c) Gizlilik: İşletme bünyesinde üretilen bilginin ve/veya üretildiği kaynağın işletme bünyesinde yetkili olmayan kişiler tarafından ulaşılmasını ve kullanılması, bilginin gizlilik kriterinin sağlanmasına olanak sağlar.

d) Bütünlük: İşletmenin iş değerleri ve beklentilerine uygunluğu sağlayacak şekilde tam ve doğru olması, bilginin bütünlük kriterini sağladığını gösterir.

e) Erişilebilirlik: İşletme bünyesinde bilgiye ihtiyaç duyulduğu zaman yetkili kişiler tarafından tam ve zamanında ulaşılabilir olmasının sağlanmasıdır.

f) Uyum: İşletme bünyesindeki iş kollarına ait iş süreçlerinin uyulması zorunlu düzenleyici otoritelere ait iş gereksinimlerine, düzenlemelere ve/veya sözleşmelere uyumlu olmasını ifade eder. Bu durum iş kolları tarafından üretilen bilginin tabi olunan düzenlemelere ve kriterlere uyumlu olmasını gerekli kılar.

g) Güvenilirlik: Yönetime; işletmeyi yönetebilmesi işletme strateji ve hedeflerini tam, doğru ve zamanında belirleyebilmesi, finansal ve diğer raporlama sorumluluklarını yerine getirebilmesi için uygun bilgilerin sağlanması gereklidir. Bu nedenle yönetime sağlanacak bilginin güvenilirliğini sağlayacak iş süreçlerinin ve bilgi alt yapısının işletme bünyesinde organize edilmesi gereklidir.

3.4 COBIT Kontrol Hedefleri

Bilgi sistemlerinin son yıllarda gelişme göstermiş olması birçok işletmede bilgi akışının bilgi teknolojileri sistemi aracılığıyla gerçekleştirilmesine neden olmuştur. Günümüzde bilgiye ulaşma zaman maliyeti çok önemli bir kriter olarak ortaya çıkmıştır. Bilginin saklanması ve bilginin en kısa zamanda ve doğru bir şekilde temin edilme isteği bilginin önemini arttırmıştır. Bu değişen koşullar nedeniyle, şirketler kendi süreçlerini, değişen ortamlara uyarlamaya çalışır. Bilgi teknolojileri ortamında bu uyarlama çabası

ile birlikte, kontrol hedeflerinin bütünü değişmese bile, bunların uygulanma şekilleri değişmektedir. Uygulama şekillerinin değişmesi, sistem üzerinde yerleştirilmiş olan iç kontrol faaliyetlerinin değerlendirilmesi yaklaşımında farklılıkların oluşmasına neden olmaktadır.

Bilgi teknolojileri ortamında, normal sistemlerde yer alan kontrol bileşenleri yer almakla birlikte, kullanılan teknolojinin niteliği, kontrol bileşenlerinin uygulanmasını etkileyebilir. Bilgi teknolojileri kontrolleri uygulandığı sistemlerde ve bilgi teknolojileri risklerini azaltmak için uygulanır. Bilgi teknolojileri kontrolleri 2 ana kategoride sınıflandırılır.

İşletme bünyesinde yer alan bilgi teknolojileri kontrollerine ait test faaliyeti; **uygunluk ve doğrulama testi** olmak üzere 2 şekilde gerçekleştirilir.

İşletme bünyesinde oluşturulan süreç dokümantasyonuna uygun bir şekilde bilgi teknolojilerine ait süreçlerin uygun bir şekilde yerine getirilip getirilmediği uygunluk testlerinde kontrol edilir. İşletme faaliyetlerinin, işletme yönetim politikaları ve prosedürleri ile uyumlu olarak gerçekleştirilip gerçekleştirilmediği uygunluk testleri ile kontrol edilir.

İşletme bünyesinde oluşturulan kontrollerin, işletme bünyesinde oluşabilecek olan usulsüz işlemlerle ilgili olarak işletmeyi hangi derecede koruyabileceğinin analizi doğrulama testleri aracılığıyla gerçekleştirilir. Doğrulama testleri kapsamında işleyen sorgulamalar, raporlama sonuçları ve kanıt toplama işlemlerini kapsamaktadır. Doğrulama testleri bilgisayar destekli denetim teknikleri ile bilgi teknolojileri denetiminden sorumlu denetçiler tarafından işletme bünyesindeki verinin kanıtlanmasına ilişkin test işlemini tam olarak gerçekleştirebilir.

Günümüzde işletmeler tarafından gerçekleştirilen kontroller değerlendirildiğinde; bilgi teknolojileri ortamında oluşturulan kontrollerin, manuel olarak gerçekleştirilen kontrol işlemlerinden daha önemli olduğu sonucu ortaya çıkmaktadır. İşletme bünyesinde oluşturulan süreçlere ait kontrollere işletme üst yönetimi ve denetim faaliyetini gerçekleştiren iç ve dış denetçiler güven duyar. Kontrollerin manuel ve/veya otomatik olması kontrollere olan güvenin derecesini değiştirmemekle birlikte, kontrol

uygulamaları sürecin niteliğine ve işlevine göre bilgi teknolojileri ortamında değişiklikler gösterebilir.

İşletme bünyesinde oluşturulan kontroller 3 ana başlık altında yer alır:[205]

1) Kurum Seviyesi Kontroller: Bu seviyede tanımlanan kontroller, ilgili kurumun kontrol ortamı içerisindeki beklentilerini gösterir. Kurum seviyesinde tanımlanan kontroller, işletmenin hedefleri ve stratejileri doğrultusunda ortaya çıkan beklentilerin hangi seviyede hayata geçirildiğinin takibi açısından kullanılır. Kurum seviyesinde tanımlanan ve uygulanan kontroller işletmenin faaliyetlerini etkin ve verimli bir şekilde yerine getirmesine destek sağlar.

2) Genel Bilgi Teknolojileri Kontrolleri: İşletme bünyesinde önleyici ve tespit edici kontroller tanımlanır ve uygulanır. Bu kontrollerin otomatik hale getirilmesinde, devamlılığının sağlanmasına katkıda bulunan kontroller genel bilgi teknolojileri kontrolleri olarak tanımlanır. İşletme bünyesindeki alt yapı kontrolleri genel kontroller olarak adlandırılır. (örn. bilgi sistemleri politikasının varlığı, erişim ve onaylama prosedürleri, değişim yönetimi, yedekleme, iş sürekliliği vb.)[206]

3) Uygulama Kontrolleri: İşletme bünyesinde gerçekleştirilen girdi, işleme (proses) ve çıkış fonksiyonlarına ait tüm kontroller uygulama kontrolleri olarak tanımlanır. Denetim türü olarak adlandırılan süreç denetimi içerisinde uygulama kontrollerinin tasarımının yanı sıra söz konusu kontrollerin etkin bir şekilde çalıştığını inceler. Uygulama kontrolleri önleyici, tespit edici ya da düzeltici olarak 3 ana başlık altında tanımlanır:[207]

- **Önleyici Kontroller:** İşletme faaliyetleri içerisinde süreç içerisinde oluşabilecek yanlışların ve hataların ortaya çıkmasını engelleyen kontrolleri ifade eder.

---

[205] Ümit Yalçın ŞEN, "Bilgi Teknolojileri Denetiminde Kontrol Tipleri", BTYD 2010, http://www.btyd.org.tr/kategori/25979-program, (28.04.2011), s.3-11.

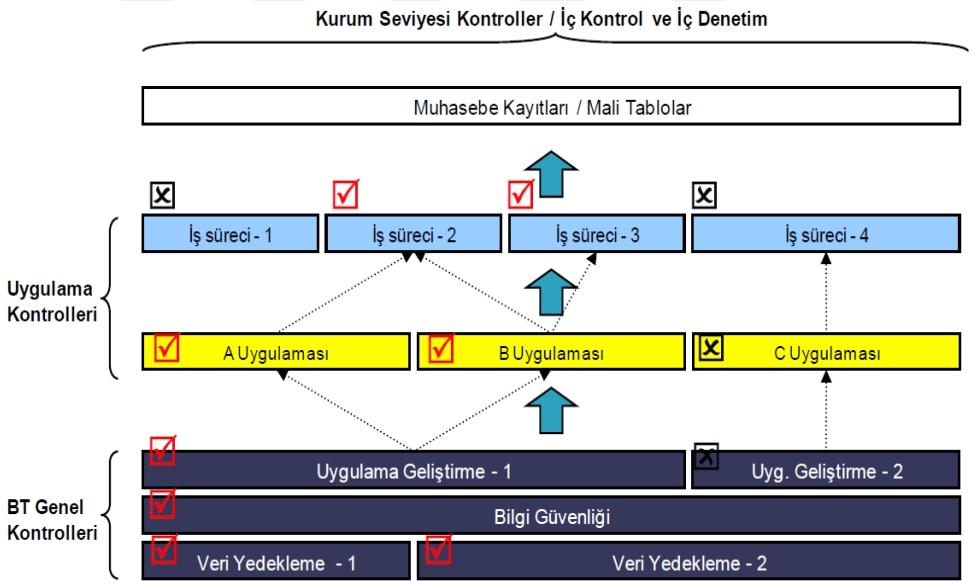
[206] Eren GEGİN, "İç Denetimde Bilgi Sistemleri Denetiminin Yeri", BTYD 2010, http://www.btyd.org.tr/kategori/25979-program, (28.04.2011), s.25.

[207] GEGİN, a.g.e., s.26.

(Örnek: Bilgi girişi sırasında bilgi girişi yapılmadan, bilginin sistem içerisinde kayıt edilmesine olanak sağlanmaması)

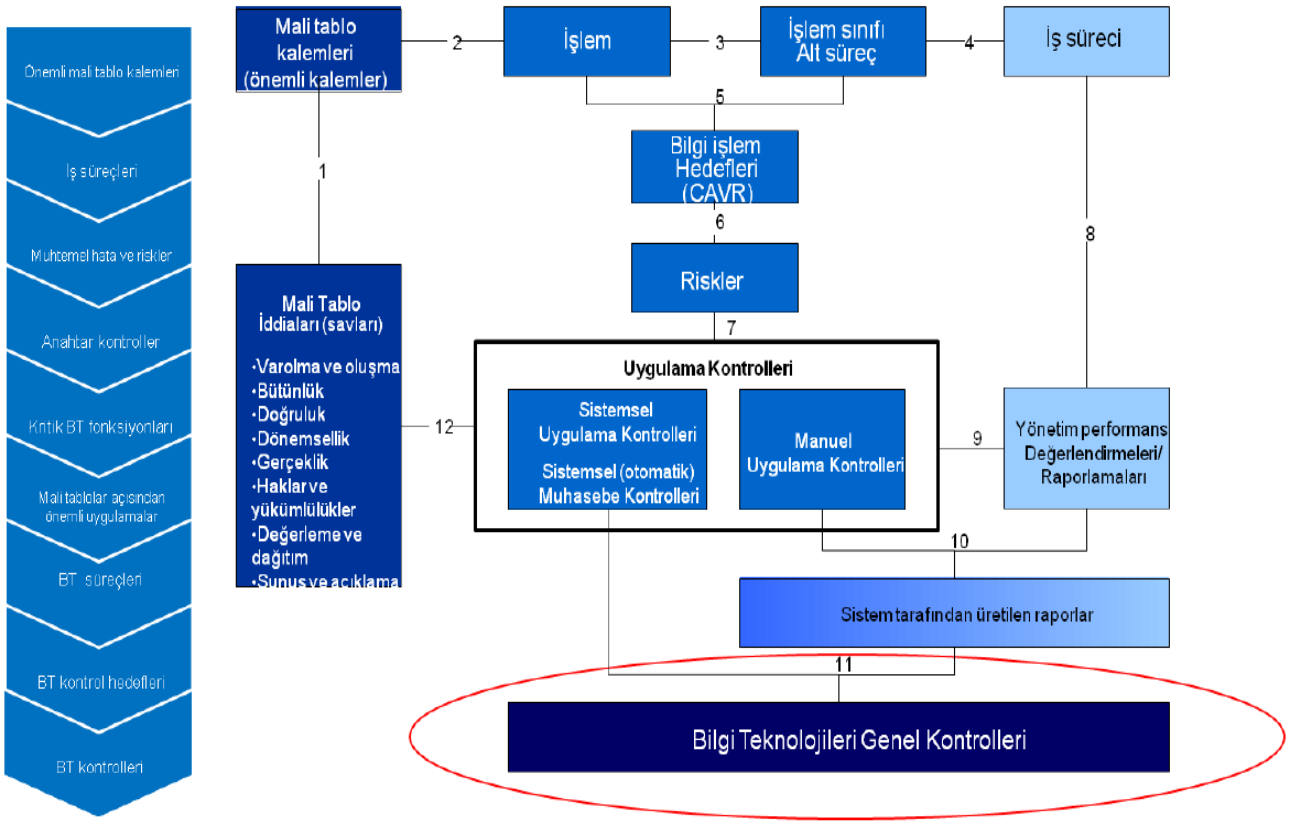
- **Tespit Edici-Belirleyici Kontroller:** Faaliyet işlemleri içerisinde yer alan önleyici kontrol proseslerine takılmamış ve/veya kontrol eksikliğinin oluşmasına istinaden oluşan hata ve/veya yanlışlıkların tespit edilmesine yönelik oluşturulan kontrolleri ifade eder. (Örnek: işletme stratejisine göre belirlenmiş olan kredi limitlerinin müşteriler tarafından aşılması durumunun tespit edilmesi vb.)

- **Düzeltici Kontroller:** Yapılan kontroller ve incelemeler kapsamında tespit edilmiş kontrol eksikliklerinin ve/veya zayıflıklarının düzeltilmesi amacıyla oluşturulan kontrol uygulamalarını ifade eder. (Örnek olarak, faaliyetlere ait sisteme girilen bilgilere ait hatalı veri girişlerinin düzeltilmesi ile ilgili olarak oluşturulan yeni kontrol uygulamaları, yetkisi olmayan kullanıcıların sisteme girişlerinin engellenmesi.)



Şekil 24: Kontrol Tipleri
Kaynak: Ümit Yalçın ŞEN, "Bilgi Teknolojileri Denetiminde Kontrol Tipleri", BTYD 2010, http://www.btyd.org.tr/kategori/25979-program, (28.04.2011), s.4.

Yukarıdaki şekilde belirtilen kontroller incelendiğinde, bilgi teknolojilerine ait kontrollerin işletme içerisindeki önemi, işlevi ve işletme içerisinde rol aldığı alanlar aşağıdaki şekil içerisinde belirtilmiştir.[208]



Şekil 25: Kontrol Tiplerinin Kurum İçerisindeki Yeri
Kaynak: Tumin GÜLTEKİN, "Finansal Denetimde İç Kontroller", BTYD 2010, http://www.btyd.org.tr/kategori/25979-program, (28.04.2011), s.8.

Kurum seviyesinde gerçekleştirilen kontroller COSO kapsamında tanımlanmış olup, bilgi teknolojileri ile ilgili olarak kontroller COBIT standardı kapsamında yer verilmiştir. **Genel ve uygulama kontrollerine** ilişkili olan ayrıntılı tanımlamalara aşağıdaki bölümlerde değinilmiştir.

[208] Tumin GÜLTEKİN, "Finansal Denetimde İç Kontroller", BTYD 2010, http://www.btyd.org.tr/kategori/25979-program, (28.04.2011), s.8.

3.4.1 Genel Kontroller

İşletme faaliyetlerinin yürütülmesinde ve bu faaliyetlerin bir sonucu olarak gerçekleştirilen finansal raporların hazırlanmasında bilgi teknolojilerine ait sistemler yaygın olarak kullanılmaktadır. Genel kontrol alanları ile ilgili olarak denetim kapsamı belirlenirken finansal verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve şirket faaliyetlerinin sürekliliğinin sağlanmasına ilişkin kontroller öncelikli olarak dikkate alınarak ilgili COBIT uygulamasında yer alan kontrol hedefleri belirlenir. Bunun yanında iş süreçlerinin önemliliği, sistem ve operasyonların maliyeti, hataların muhtemel sonuçlarının şirkete ve finansal raporlamalara olumsuz etkisinin büyüklüğüne göre kontroller belirlenebilir.

Genel kontroller, bilgi teknolojileri ile ilgili politikalar, prosedürler ve işleyen pratiklerden herhangi birini içeren, işletmenin bilgi teknolojileri alt yapısı, bunun planlanması, organizasyonu, bilgi teknolojileri kaynaklarına yönelik gerçekleştirilecek satın almalar, temin edilen kaynakların uygulanması, hizmet sunumu, sunulan hizmetlerin devamlılığının sağlanması için gereklilikler ve bilgi teknolojileri işlemlerinin izlenmesine ve değerlendirilmesine yönelik faaliyetler ile ilgilenir. Genel kontroller, ayrı sorgulama teknikleri veya belirli bir hesaplama yöntemlerine veya finansal uygulamalara göre kesinlik göstermemektedir. Birçok uygulamada, bilgi teknolojileri değerlendirmesinin genel kontrol elemanları, işletmenin bilgi teknolojileri bölümü üzerinde yoğunlaşır. Temel olarak aşağıdaki belirtilen 8 temel kontrol ile COBIT uygulamasının 4 temel alanı dikkate alınır. COBIT uygulaması, dört süreç alanında gruplanmış 34 bilgi teknolojisi sürecini ele alır. Bu dört grup;

1) Planla ve organizasyon

2) Tedarik ve uygulama

3) Hizmet sunumu ve destek

4) İzleme ve değerlendirme

şeklindedir.

Aşağıdaki başlıklar içerisinde COBIT genel kontrol tanımlamalarının ayrıntısı açıklanmış olup, açıklamalar kapsamında bankacılık sektöründeki uygulamasına değinilmiştir.

3.4.1.1 Planlama ve Organizasyon

Planlama ve organizasyon (PO) faaliyetleri, iş hedeflerinin yerine getirilmesini amaçlar. Bu amaç kapsamında bilgi teknolojileri desteğinin en uygun şekilde yerine getirilmesi ile ilgili strateji ve yöntemleri içerir. Stratejiler; farklı bakış açılarını içerecek şekilde planlanır. Belirlenen strateji ve yöntemler, organizasyon içerisindeki ilgili bölüm ve çalışanlara duyurulur. Bilgi sistemleri denetimi kapsamında; işletmenin kullandığı bilgi teknolojileri alt yapısının, uygun bir organizasyonel kurgu kapsamında işletmeye katkı sağlayacak şekilde çalışıp çalışmayacağı durumu dikkate alınır.

Banka yönetimi açısından değerlendirildiğinde; planlama ve organizasyon faaliyeti oluşturulan strateji ve stratejilere göre uygulanması gereken taktikleri kapsar. Bu aşamada banka stratejilerine ulaşmada en iyi katkının sağlanması için hangi faaliyetlerin gerçekleştirilmesi gerektiği tanımlanır. İşletme hedeflerine bağlı olan ve işletmeye yön veren işletme bakış açısı birçok ihtiyacı ortaya çıkarabilir. Bunlar; farklı bir şekilde planlamanın oluşturulması, iletişim kurma ve yönetim ihtiyacının ortaya çıkmasına neden olur. Bu nedenle banka bünyesinde belirlenen hedefler ve stratejiler dikkate alınarak teknolojik altyapı ile birlikte uygun bir organizasyon yapısı oluşturulmalıdır. Bu faaliyet, üst yönetim tarafından aşağıdaki belirtilen konuların sorgulanmasına neden olur. Bu konular:

- Banka stratejisi ile bilgi teknolojileri tarafından belirlenen stratejiler, uyumlu mu?

- Banka içerisindeki mevcut kaynaklar ideal ve verimli bir şekilde kullanılıyor mu?

- Banka içerisinde yer alan organizasyondaki çalışanlara bilgi teknolojilerine ait hedefler bilgilendirilmiş mi? Söz konusu teknolojik hedefler çalışanlar tarafından anlaşılıyor ve benimseniyor mu?

- Bilgi teknolojilerine ait riskler tespit edilmiş, belirlenmiş ve tanımlanmış mı?

- Bilgi teknolojilerine ait riskleri minimize edecek şekilde riskler yönetiliyor mu?

- Banka ihtiyaçları doğrultusunda bilgi teknolojilerine ait oluşturulan sistemler ihtiyacı karşılıyor mu?

Planlama ve organizasyon faaliyetine ilişkin genel kontroller kapsamında;

✓ Bilgi teknolojilerine ait stratejik planlama tanımının yapılması,

✓ Tanımlanan stratejik planlamaya uygun olarak bilgi mimarisinin tanımlanması,

✓ İşletme bünyesinde teknolojik değişiklik ve gelişime yönelik ilerleme hedefinin belirlenmesi,

✓ Bilgi teknolojileri alt yapısına ait süreçlerin, organizasyon yapısının ve organizasyonuna ait bağlantıların tanımlanması,

✓ Bilgi teknolojilerine ait yapılan yatırımların yönetimi,

✓ Yönetimin amaçlarının ve talimatlarının iletilmesi,

✓ İnsan kaynakları yönetimi,

✓ Kalite yönetimi,

✓ Bilgi sistemlerine ait risklerin değerlendirilmesi ve yönetimi,

✓ Bilgi teknolojileri ile ilgili olarak yapılması planlanan ve/veya yapılan projelere ait proje yönetimi,

Faaliyetleri ve/veya iş akışları ile ilgili olan kontrol hedefleri değerlendirilir ve incelenir.

Planlama ve organizasyon kriteri içerisinde 10 adet alt faaliyet bulunmaktadır. Bu faaliyetler:

PO1 Stratejik Bilgi Teknolojileri Planının Tanımlanması

PO2 Bilgi Mimarisi Tanımlaması

PO3 Teknolojik Yön Kararı

PO4 Bilgi teknoloji süreçlerinin, organizasyonunun ve ilişkilerinin tanımlanması

PO5 Bilgi teknolojilerine ait yatırımların yönetilmesi

PO6 Yönetimin amaçlarının ve talimatlarının iletilmesi

PO7 İnsan kaynakları yönetimi

PO8 Kalite yönetimi

PO9 Bilgi sistemleri risklerinin değerlendirilmesi ve yönetimi

PO10 Proje yönetimi

3.4.1.2 Tedarik ve Uygulama

Tedarik ve uygulama (AI[209]) faaliyetleri, bilgi teknolojisi stratejilerinin oluşturulması ve uygulanması ile ilgilidir. Bu faaliyet kapsamında; bilgi teknolojisi çözümleri tanımlanır. Yapılan tanımlama kapsamında bilgi teknolojisi çözümlerinin geliştirilmesini veya dış destek sağlayıcılardan temin edilmesini, uygulanmasını ve iş süreçleriyle bütünleştirilmesini kapsar. İşletmenin kullandığı bilgi teknolojileri sistemlerindeki bakım ve değişiklik işlemleri bu kontrol faaliyeti alanında incelenir ve değerlendirilir.

İşletmenin belirlemiş olduğu bilgi teknolojilerine ait stratejilerinin faaliyete geçirilmesi amacıyla; bilgi teknolojisi işlemlerine ait sonuçların iş süreçlerine

[209] AI: Acquire and Implement

uygulanması gereklidir. Bu amaç kapsamında bilgi teknolojisi işlemlerine ait sonuçların iş sonuçları ile bütünleştirilmesine, tanım kapsamında birlikte değerlendirilmesine, geliştirilmesine ya da temin edilmesi gereklidir. İşletme hedeflerinin bilgi teknolojilerinde yer alan çözümlerle karşılanması sağlanmalıdır. Bu kapsamda, işletme bünyesinde yer alan sistemlerin korunması ve değiştirilmesi işlemleri bu alanda değerlendirilir. Değerlendirme kapsamında, üst yönetim tarafından aşağıdaki belirtilen konuların sorgulanması sağlanır:

- İşletme bünyesinde kullanılan bilgi teknolojilerinde oluşturulan yeni projelerin, işletme içerisindeki iş kollarına ait iş ihtiyaçlarını karşılayacak çözümleri ortaya koyabilir mi?

- İş ihtiyaçlarının karşılanabilmesi amacıyla uygulanması hedeflenen yeni projelerin, önceden belirlenmiş olan bütçe kapsamında tam, doğru, zamanında ve istenen kalite kapsamında gerçekleştirilme olasılığı var mı?

- Yeni bilgi teknolojileri projeleri kapsamında işletme bünyesinde oluşacak olan yeni değişimler mevcut durumda yürütülen iş süreçlerini olumsuz yönde etkileyecek mi?

Tedarik ve uygulama faaliyeti ile ilgili olan genel kontroller kapsamında;

✓ İşletme içerisinde kullanılan otomasyon çözüm sistemlerinin tanımlanması ve tespit edilmesi,

✓ İşletme bünyesinde teknolojik gelişmelere bağlı olarak ve/veya işletme ihtiyaçları doğrultusunda geliştirilen uygulama yazılımları ve bakım faaliyetleri,

✓ İşletme içerisinde oluşturulmuş olan ve/veya güncellenen teknolojik altyapının incelenmesi ve bakımı,

✓ Yürütülen işlemlere ait faaliyet organizasyonun sağlanması ve kullanım işleminin etkinliğinin sağlanması,

✓ Bilgi sistemleri kaynaklarının temin edilmesi,

- ✓ Bilgi teknolojileri iş sürekliliği ve değişim yönetimi,
- ✓ Sistem sorunlarına ait problemlerin giderilmesi ve sistem içerisinde yapılan değişikliklerin uygulanması ve uygulama standartlarının belirlenmesi,

Başlıklarına ait kontrol hedefleri incelenir ve gözden geçirilir.

Tedarik ve uygulama kontrol hedefi içerisinde 7 adet alt faaliyet bulunur. Bu faaliyetler:

AI1 Otomasyon çözümlerinin belirlenmesi

AI2 Uygulama yazılımının geliştirilmesi ve bakımı

AI3 Teknoloji altyapısının elde edilmesi ve bakımı

AI4 Operasyona olanak sağlama ve kullanma

AI5 Bilgi teknolojileri kaynaklarını tedarik etme

AI6 Değişiklik yönetimi

AI7 Sistem çözümlerinin, değişikliklerinin uygulaması ve akredite edilmesi

3.4.1.3 Hizmet Sunumu ve Destek

Hizmet sunumu ve destek (DS[210]) faaliyetleri, işletme tarafından operasyonel işlemlerini yerine getirebilmesi amacıyla ihtiyaç duyduğu hizmetlerin, eğitim faaliyetleri ile birlikte güvenli ve sürekli olarak temin edilmesidir.

Bu faaliyet alanı, hizmet sunumu, güvenlik ve devamlılığın yönetimi, kullanıcılar için servis desteği ve oprasyonel fırsatlar ile veri yönetimi içeren gerekli hizmetlerin ortaya konulmasıyla ilgilenir. Bu faaliyet kapsamında üst yönetim tarafından aşağıdaki belirtilen konular sorgulanır:

[210] DS: Deliver and Support

- Bilgi teknolojisi hizmetleri iş önceliklerini dikkate alarak uyumlu bir şekilde uygulanabilir mi?

- Bilgi teknolojileri ile ilgili olarak işletme bünyesinde gerçekleştirilen harcamalar optimize edilebilir mi?

- Bilgi teknolojilerine ait ortaya konulan sistemler, işletme bünyesinde görev alan mevcut iş gücü tarafından verimli ve güvenli bir şekilde uygulanabilir mi?

- Mevcut durumda işletme bilgilerinin bulunduğu sistem içerisinde bilgi güvenliği ile ilgili olarak yeterlilik, gizlilik, bütünlük ve elverişlilik bulunuyor mu?

Hizmet sunumu ve destek faaliyetlerine ilişkin genel kontroller çerçevesinde;

✓ Hizmet pozisyonlarının ve düzeylerinin belirlenmesi, tanımlanması ve yönetilmesi,

✓ İşletme dışındaki kaynaklardan temin edilen hizmet faaliyetlerinin organize edilmesi ve yönetimi,

✓ Performans ve kapasite yönetimi,

✓ Sunulan ve/veya sunulacak olan hizmet devamlılığının sağlanması,

✓ Sistem güvenliğinin sağlanması,

✓ Hizmet sunumu ve destek faaliyetleri ile ilgili olarak oluşan maliyet kalemlerinin tanımlanması ve gerekli olan masraf dağılımlarına aktarılması,

✓ Hizmet verilen kullanıcıların eğitilmesi,

✓ Hizmet sunumu yönetimi ve olay yönetimi,

✓ Konfigürasyon yönetimi,

✓ Problem yönetimi,

✓ Veri yönetimi,

- ✓ Fiziksel çevre yönetimi,
- ✓ Operasyon yönetimi,

Süreçleri ile ilgili kontrol hedefleri incelenir ve değerlendirilir.

Hizmet sunumu ve destek faaliyeti içerisinde 13 adet alt faaliyet yer alır. Bu faaliyetler:

DS1 Hizmet seviyelerini tanımlama ve yönetme

DS2 Üçüncü şahıs hizmetlerinin yönetimi

DS3 Performans ve kapasite yönetimi

DS4 Hizmet sürekliliğinin sağlanması

DS5 Sistem güvenliğinin sağlanması

DS6 Giderlerin tanımlanması ve paylaştırılması

DS7 Kullanıcıların eğitilmesi

DS8 Hizmet masasının ve problemlerin yönetilmesi

DS9 Konfigürasyon yönetimi

DS10 Problem yönetimi

DS11 Veri yönetimi

DS12 Fiziksel çevre yönetimi

DS13 Operasyon yönetimi

3.4.1.4 İzleme ve Değerlendirme

İzleme ve değerlendirme faaliyetleri (ME[211]), bilgi teknolojileri kontrollerinin kalitesinin ve uygunluğunun, denetim faaliyetini gerçekleştiren denetçi tarafından belirlenen periyot kapsamında düzenli olarak değerlendirme yapmasını ifade eder.

Değişen koşullara ve iş ihtiyaçlarına bağlı olarak işletme bünyesinde yer alan bütün bilgi teknolojisi işlemlerinin, geçen süre içerisindeki hizmet kaliteleri ve verimlilikleri düzenli bir şekilde değerlendirilmelidir. İzleme ve değerlendirme faaliyeti, performans yönetimi, iç kontrolün izlenmesi, mevzuat uyumu ve yönetime bilgi verilmesi gibi işlemleri içerir. Bu faaliyet içerisinde, üst yönetim tarafından aşağıdaki belirtilen hususlar sorgulanır. Bunlar:

- Bilgi teknolojilerinin performansı periyodik olarak değerlendiriliyor mu? Periyodik değerlendirme faaliyeti yaşanabilecek olan problemleri önceden tespit edebilecek nitelikte mi?

- İşletme yönetimi tarafından işletme içerisindeki iç kontrol faaliyetinin etkili ve verimli olmasını sağlayabiliyor mu?

- İşletme içerisindeki bilgi teknolojisi performansı, geçmişte belirlenen işletme hedefleri ile ilişkili mi?

- Bilgi güvenliği için mevcut durumda yeterli gizlilik, bütünlük ve elverişlilik var mı?

İzleme ve değerlendirme faaliyetine ilişkin kontroller kapsamında;

✓ Bilgi sistemlerine ait gerçekleştirilen işlem ve faaliyetlere ait performans bilgilerinin izlenmesi ve değerlendirilmesi,

✓ İç kontrol yapısının izlenmesi ve değerlendirilmesi,

[211] ME: Monitor and Evaluate

✓ Denetlenenin işletme içi yönetmelik ve kriterler kapsamında, uygulanması gereken mevzuat kriterlerine uyum sağlaması,

✓ Bilgi sistemleri bünyesinde uygulanacak olan kurumsal yönetişim standardının sağlanması ile ilişkili olan kontrol kriterleri kontrol edilir ve değerlendirilir.

İzleme ve değerlendirme faaliyeti 4 adet alt faaliyetten oluşmaktadır:

ME1 Bilgi teknolojileri performansının izlenmesi ve değerlendirilmesi

ME2 İç kontrolün izlenmesi ve değerlendirilmesi

ME3 İşletme dışı koşullarla uyumun sağlanması

ME4 Bilgi teknolojileri yönetiminin sağlanması

3.4.2 Uygulama Kontrolleri ve Sınıfları

Uygulama kontrolleri bilgi sistemleri kapsamında bulunan ve işletme operasyonlarını gerçekleştirebilmek için kullanılan verilerin tanımlanması, üretilmesi, kullanılması, güvenilirlik ve bütünlüğünün sağlanması, verilere erişimin yetkilendirilmesi, kimlik doğrulamasının tam olmasına, sorgulamaların geçerli olmasına ve diğer çeşitli veri girişine yardımcı olan kontrolleri içerir. Uygulama kontrollerinin amacı;[212]

1) Sisteme girilen verinin doğru, tam, bütün ve yetkili kişiler tarafından oluşturulduğundan,

2) İşletme bünyesinde faaliyet sonuçlarına göre oluşan verilerin işletme bünyesinde önceden kabul edilmiş niteliklerde ve süre dahilinde sisteme girişinin yapıldığından ve işlendiğinden,

[212] Christine BELLINO, Jefferson WELLS, Steve HUNT ve Crowe HORWARTH LLP, **Global Technology Audit Guide (GTAG) 8: Auditing Application Controls**, The Institute of Internal Auditors, January 2009, s.2.

3) Sistem içerisinde yer alan verilerin doğru ve eksiksiz bir şekilde saklandığından,

4) Verilere bağlı olarak oluşan çıktı verilerinin tam, doğru ve eksiksiz olduğundan emin olmaktır.

Uygulama kontrolleri kapsamında, geçersiz veri girişlerinin kontrol edilmesi için, kullanıcı tarafından girilen verinin sistem tarafından kontrol edilmesi, belirli sorgulamaları gerçekleştirebilecek olan personel sorgulamalarının sistem tarafından kontrol edilmesi, tüm sorgulamaların tam, doğru ve zamanında yapıldığının kontrol edilmesi için yapılan sorgulama kontrolleri, uygulama kontrollerine örnek olarak gösterilebilir. Özet olarak uygulama kontrolleri, denetim çalışması uygulanan iş süreçlerinin kontrolünü ifade eder. Uygulama kontrolleri; faaliyet kontrolleri içerisinde bulunan, bilgi sistemleri destekli ve/veya manuel işlemlerle gerçekleştirilen özelleşmiş kontrollerdir. Uygulama kontrolleri bünyesinde **giriş, çıkış, işleme ve sınır kontrollerini** içerir.

1 Kasım 2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik" genel olarak denetlenecek uygulama kontrollerini sınıflandırarak, bağımsız denetim faaliyetini gerçekleştiren bağımsız denetim firmasının da bu sınıflandırmaya uygun olarak ilgili kontrolleri yasal kuruma ("BDDK") raporlamasını talep etmektedir. Uygulama kontrolleri sınıflandırılması yapılırken COBIT uygulamasının ön gördüğü yaklaşım dikkate alınmıştır.

Uygulama kontrolleri sınıflandırılması kapsamında BDDK tarafından bankaların asgari olarak denetlenmesi gereken iş süreçleri aynı yönetmelik içerisinde belirtmiştir.

COBIT uygulamasının referans olarak alındığı BDDK yönetmeliğinde, bankalarda gerçekleştirilen faaliyetlere ait süreçlerle ilgili olarak, aşağıdaki uygulama kontrolleri belirlenmiştir. Yönetmelik kapsamında belirlenen kontrollerin test edilip, değerlendirilmesi gerektiği belirtilmiştir. Kontrollerin test edilmesi ile ilgili olarak bazı

kontrol sınıfları belirlenmiş; değerlendirme ve test yaklaşımının ne şekilde uygulanması gerektiği belirtilmiştir.[213]

a) Veri oluşturma/yetkilendirme kontrolleri: Bu kontroller, bilgi sistemleri içerisinde yer alan kaynak veri, belgelerin oluşturulması ile bilgi sistemleri içerisindeki yetkilendirme faaliyetinin gerçekleştirilmesi ile ilgilidir. Bu kontrol içerisinde kontrol tipleri yer alır. Kontrol tipleri beş ayrı kategoriye bölünmüştür. Bunlar;[214]

1. Veri hazırlama prosedürleri

2. Kaynak belge yetkilendirme prosedürleri

3. Kaynak belge verilerinin toplanması

4. Kaynak belgelerdeki hata ve yanlışlıkların değerlendirilmesi

5. Kaynak belgelerin muhafaza edilmesi

b) Girdi kontrolleri: Bilgi sistemleri verilerinin işlenmesine yönelik ilgili sürecin başlangıcı olan girdi sürecine ait yapılan kontrol işlemlerini ifade eder. Bu kontroller, üç ayrı kategoride sınıflandırılır:[215]

1. Girdi yetkilendirme prosedürleri
2. Doğruluk, bütünlük ve yetkilendirme kontrolleri
3. Veri girdilerindeki hataların ele alınması

c) Veri işleme kontrolleri: Bilgi sistemleri içerisinde veri işleme süreci ile ilgili sınıflandırılan üç ayrı kategorideki kontrollerdir. Bunlar;[216]

1. Veri işlemede bütünlük
2. Veri işlemede onaylama ve değiştirme

---

213 BDDK, "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik", Madde 18, Sayı 26170, Tarih: 16 Mayıs 2006, s.8-9.

214 ISACA, "Control Objectives for Information and related Technology 4.0 (USA)", 2005, s.17.

215 ISACA, a.g.e., s.17.

216 ISACA, a.g.e., s.18.

3. Veri işlemedeki hataların ele alınması

d) Çıktı kontrolleri: Bilgi sistemlerinde veri girişinin ve veri işleme aşamaları oluştuktan sonra ortaya çıkan veri üzerinde uygulanan kontrollerdir. Çıktı kontrolleri değerlendirirken 5 ayrı kontrol tipi kontrol edilir.[217]

1. Çıktıların temin edilmesi ve saklanması
2. Çıktıların dağıtımı ve dağılımı
3. Temin edilen çıktıların uyumluluğu ve üçüncü taraflar ile mutabakatı
4. Çıktıların gözden geçirilmesi ve hataların ele alınması
5. Çıktı raporlarının güvenliğinin sağlanması

e) Sınır kontrolleri: İşletme organizasyon yapısı dışından elde edilen verinin, organizasyonun ihtiyaçlarına olan uygunluğunun ve bütünlüğünün sağlamasına yönelik olarak yapılan kontrolleri ifade eder. Sınır kontrolleri içerisinde önem derecesi yüksek olan bilginin güvenli olarak iletilmesi ve korunması hedeflenir. Sınır kontrolleri toplam 2 kategoride sınıflandırılmıştır.[218]

1. Verinin aslına uygunluğu ve bütünlüğüne yönelik kontroller
2. Önemli olarak sınıflanan bilginin iletim ve transfer aşamasında korunması

BDDK'nın oluşturduğu yönetmelik hazırlanırken, COBIT uygulamasının dördüncü versiyonu baz alınmıştır. Yukarıdaki yer alan kontrol çeşitlerine ait sınıflandırma COBIT uygulamasının 4.1 versiyonunda uygulama kontrolleri sadece altı çeşit olarak sınıflandırılmıştır. Yeni sınıflandırma yaklaşımı, uygulama kontrollerine ait takip edilebilirlik fonksiyonunu daha kolay bir hale getirmiştir. Yeni sınıflandırmaya göre kontrol çeşitleri aşağıdaki gibi sınıflandırılmıştır:[219]

---

[217] Cengiz GÜNEY, "Bilgisayarlı Muhasebe Sistemlerinde Denetim Riskleri ve Bilgisayar Destekli Denetim Teknikleri", **Akademik Sosyal Araştırmalar Dergisi**, Sayı:28, Temmuz 2016, s.353.

[218] ISACA, a.g.e., s.18.

[219] ISACA COBIT, a.g.e., s.16.

1) Kaynak Veri Hazırlama ve Yetkilendirme: İşletme faaliyetlerinin yerine getirilmesine imkân sağlayan kaynak dokümanların yetkili ve yetkin kişiler tarafından işletme bünyesinde tanımlanan prosedürlerin kullanılmasıyla hazırlanmasını sağlayan kontrolleri ifade eder. Yetkili ve yetkin kişiler tarafından gerçekleştirilen işlemlere ait süreçler içerisinde görevler ayrılığı prensibinin de göz önünde bulundurulması gerekir. Bu işlem kapsamında veri hazırlama ve onaylama işlemlerinin birbirinden ayrılması beklenmektedir. Belirtilen bu kontroller, temin edilen kaynak verilerin tam, doğru ve zamanında hazırlanmasına ve ilgili süreç içerisinde oluşabilecek olan hata ihtimallerinin raporlanmasını sağlar.

2) Kaynak Veri Toplama ve Girişi: İşletme bünyesinde kullanılan sistemlere veri girişlerinin yetkin ve yetkili kişiler tarafından yapılmasını sağlayan kontrolleri ifade eder. Örneğin bankacılık uygulamasında mevduat faizlerinin iki ayrı kişi tarafından sisteme doğru girilmesi ile sistemde kullanılabilir hale gelmesi belirtilen kontrollere örnek olarak verilebilir.

3) Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri: Sistem üzerindeki verilerin doğru, tam ve geçerli olmasını sağlayan kontrollerdir. Veri girişi sırasında geçerlilik kontrolü yapılması veya sistem üzerinde uygun yetkilendirmenin yapılması gibi kontroller bu kategori içerisinde yer alır. Müşteri bilgilerinin sisteme girişi esnasında adres bilgisinin sisteme girilirken il seçimine göre uygun ilçelerin seçilmesinin sistem tarafından zorlanması, bu kontrol sınıfına örnek olarak verilebilir.

4) Veri İşlemede Bütünlük ve Geçerlilik: İşletme bünyesinde yer alan sistem tarafından veri işleme aşamasında, işlenen verinin bütünlüğünün ve geçerliliğinin sağlanmasına yönelik kontrollerdir. İşletme içerisinde kullanılan sistemler üzerinde çalışan programların hatalı işlem girişlerini belirlemesi ve veri işleme süreci tamamladığında ayrı olarak raporlamasına ait kontroller, bu kontrol sınıfına örnek olarak gösterilebilir.

5) Çıktıların Gözden Geçirilmesi, Mutabakat ve Hataların Ele Alınması: Sınıflanan bu kontrol başlığı altında, sistem içerisinden temin edilen çıktı raporlarının doğruluğunun, çıktı bilgilerini sağlayan kullanıcılar ve yetkilendirilmiş olan kullanıcılar

tarafından gözden geçirilmesi ve mutabakatının temin edilmesini sağlayan kontrollere yer verilir. Bu faaliyetlerin yanında temin edilen çıktılarda yer alan hataların belirlenmesi ve tanımlanmasına ait diğer kontroller de bu kapsam içerisinde değerlendirilir. EFT işlemlerinin gün sonu mutabakatlarının bankalar tarafından yapılması bu kontrol sınıfı için bir örnek oluşturmaktadır.

6) İşlemlerin Yetkilendirilmesi ve Bütünlük: İşlemlerin ve dolayısıyla verinin sistemlere ait ara yüzler ve fonksiyonlar arasından iletilirken bütünlüğünün sağlanmasına ve işlemlerin belirlenen yetkiler çerçevesinde gerçekleşmesine yardımcı olan kontrollerdir. Örneğin, internet bankacılığı ön yüzünden gerçekleştirilen işlemin arka taraftaki ana bankacılık sisteminde bütünlüğü bozan bir işlem olması sebebiyle sistem tarafından gerçekleştirilmesine izin verilmemesi gibi.

Denetim faaliyetini gerçekleştiren gerek bağımsız denetim kuruluşu gerekse banka içerisindeki bilgi teknolojileri denetçileri, bilgi teknolojileri denetimi kapsamında uygulama kontrollerinin denetlenmesinde aşağıdaki yer alan koşulları mutlaka yerine getirmelidir:

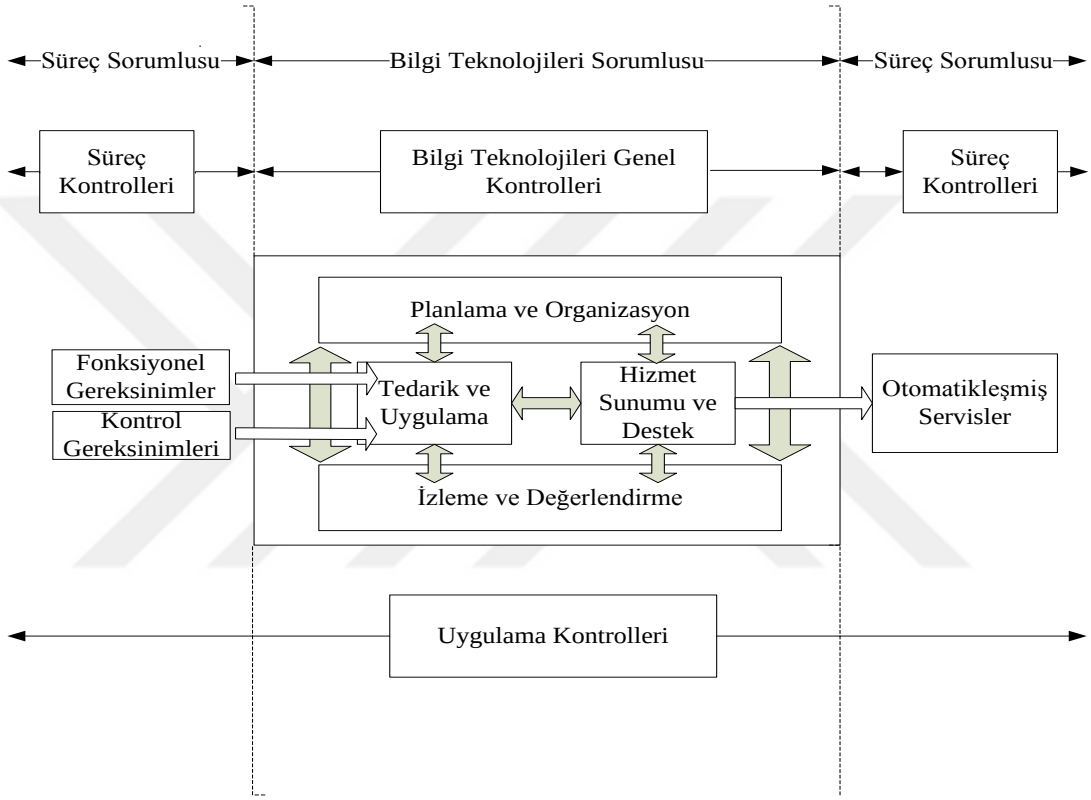
- Önemli uygulama bileşenlerinin ve işlem hareketlerinin tespit edilmesi, söz konusu uygulama bileşen ve işlemlerinin sistem içerisindeki iş ve bilgi akışına ait tanımlamalarının yapılması, işlemlere ait oluşturulmuş olan güncel dokümantasyonların incelenmesi ve süreç sahibi yetkin personellerle sürecin değerlendirilerek uygulamaya ait ayrıntıların temin edilmesi,

- Bilgi sistemleri içerisinde yer alan ve uygulanan uygulama kontrollerinin etkin ve etkili olduğu alanların belirlenmesi ve belirlenen alanlarla ilgili olan kontrol eksikliklerinin yapılması öngörülen test işlemlerine ve stratejilerine olan etkisinin gözden geçirilmesi,

- Banka bünyesinde yapılacak olan denetim kapsamında uygun ve etkili olan denetim proseslerinin kullanılarak, faaliyetler kapsamında oluşturulmuş olan kontrollerin verimliliklerinin ve etkinliklerinin test edilmesi ve değerlendirilmesi,

- Denetim çalışması kapsamında yapılan test işlemlerine ait sonuçların ve diğer denetim tespitlerinin incelenmesi ile birlikte, uygulanan kontrol ortamının değerlendirme işlemleri uygulanmalıdır.

COBIT 4.1 versiyonu uygulamasında kontrollerin birbirleri ile olan ilişkileri ve sınırları aşağıdaki yer alan şekil içerisinde açıklanmaya çalışılmıştır.[220]



Şekil 26: COBIT Kontrolleri Arasındaki Bağlantı
Kaynak: ISACA, "COBIT 4.1 Framework Control Objectives Management Guidelines Maturity Models", 2007, s.15.

[220] ISACA, COBIT 4.1, a.g.e., s.16.

3.5 COBIT ve COSO Bileşenleri Arasındaki İlişki

Yukarıdaki başlıklar içerisinde COBIT bileşenleri tanımlanmıştır. Bu başlık kapsamında, birinci bölüm içerisinde yer alan COSO bileşenleri ile COBIT bileşenleri arasındaki bağlantı anlatılacaktır.

COBIT uygulamaları genel olarak bilgi teknolojileri yönetişiminin uygulanması ile ilgili bileşenlerin bütününü oluşturur. COBIT uygulamalarının, COSO kontrol bileşenleri ile direkt olarak ilişkisi bulunmaktadır.

COBIT uygulamaları ISACA[221] tarafından yönetilmekle birlikte bilgi teknolojileri uygulamalarındaki riskleri ve kontrolleri; 4 ana bileşen altında, 318 detaylı kontrol hedefi ve 34 bilgi teknolojisi bileşenleri ile yönetir. COBIT bileşenleri uygulama ve kurum düzeyinde olmak üzere iki farklı şekilde değerlendirildiğinde; aşağıdaki tablo ortaya çıkar.

[221] ISACA: The Information Systems Audit and Control Association

Tablo 3: COBIT ve COSO Bileşenleri Arasındaki İlişki

Referans	Kurum Düzeyi	Aktivite Düzeyi	COBIT Bilgi Teknolojileri Süreçleri	COSO BİLEŞENLERİ				
				Kontrol Ortamı	Risk Değerlendirme	Kontrol Faaliyetleri	Bilgi ve İletişim	İzleme
PO	**Planlama ve Organizasyon (Bilgi Teknolojileri Ortamı)**							
PO1	◆		Stratejik Bilgi Teknoloji Planının Tanımlanması		◆		◆	◆
PO2			Bilgi Mimarisi Tanımlaması					
PO3			Teknolojik Yön Kararı					
PO4	◆		Bilgi Teknoloji Süreçlerinin, Organizasyonunun ve İlişkilerinin Tanımlanması	◆			◆	◆
PO5			Bilgi Teknolojilerine ait Yatırımların Yönetilmesi					
PO6	◆		Yönetimin Amaçlarının ve Talimatlarının İletilmesi	◆			◆	
PO7	◆		İnsan Kaynakları Yönetimi	◆			◆	
PO8	◆		Kalite Yönetimi	◆		◆	◆	◆
PO9	◆		Bilgi Sistemleri Risklerinin Değerlendirilmesi ve Yönetimi		◆			
PO10			Proje Yönetimi					
AI	**Tedarik ve Uygulama (Program Geliştirme ve Program Değişikliği)**							
AI1			Otomasyon Çözümlerinin Belirlenmesi					
AI2		◆	Uygulama Yazılımının Geliştirilmesi ve Bakımı			◆		
AI3		◆	Teknoloji Altyapısının Elde Edilmesi ve Bakımı			◆		
AI4		◆	Operasyona Olanak Sağlama ve Kullanma			◆	◆	
AI5			IT Kaynaklarını Tedarik Etme					
AI6		◆	Değişiklik Yönetimi		◆	◆		◆
AI7		◆	Sistem Çözümlerinin ve Değişikliklerinin Uygulaması ve Akredite Edilmesi			◆		
DS	**Hizmet Sunumu ve Destek**							
DS1		◆	Hizmet Seviyelerini Tanımlama ve Yönetme	◆		◆	◆	◆
DS2		◆	Üçüncü Şahıs Hizmetlerinin Yönetimi	◆	◆	◆		◆
DS3			Performans ve Kapasite Yönetimi					
DS4			Hizmet Sürekliliğinin Sağlanması					
DS5		◆	Sistem Güvenliğinin Sağlanması			◆	◆	◆
DS6			Giderlerin Tanımlanması ve Paylaştırılması					
DS7	◆		Kullanıcıların Eğitilmesi	◆			◆	
DS8		◆	Hizmet Masasının ve Problemlerin Yönetilmesi			◆	◆	◆
DS9		◆	Konfigürasyon Yönetimi			◆	◆	

DS10		◆	**Problem Yönetimi**			◆	◆	◆
DS11		◆	**Veri Yönetimi**			◆	◆	
DS12		◆	**Fiziksel Çevre Yönetimi**			◆	◆	
DS13		◆	**Operasyon Yönetimi**			◆	◆	
ME	**İzleme ve Değerlendirme**							
ME1	◆		**Bilgi Teknolojileri Performansının İzlenmesi ve Değerlendirilmesi**			◆	◆	◆
ME2	◆		**İç kontrolün İzlenmesi ve Değerlendirilmesi**	◆				◆
ME3	◆		**İşletme Dışı Koşullarla Uyumun Sağlanması**			◆	◆	◆
ME4	◆		**Bilgi Teknolojileri Yönetiminin Sağlanması**	◆				◆

Kaynak: IT GOVERNANCE INSTITUTE, **"IT Control Objectives for Sarbanes-Oxley: The Role of IT In The Design and Implementation of Internal Control Over Financial Reporting"**, 2nd Edition, USA, September 2006, s.56.

Günümüzde bankalar tarafından yürütülen operasyonların birçoğu bilgi teknolojileri sistemleri aracılığıyla gerçekleştirilir. Bankacılık sistemleri içerisinde yer alan bilgiler, bilgi talep eden taraflara bilgi sistemleri aracılığıyla raporlanmaktadır. Bu sistemler, kurumsal kaynak planlama sistemleri ve/veya başka bir sistem olmakla birlikte yetkilendirme, kayıt, işleme ve finansal işlemlerin raporlama işlemleri ile derinlemesine entegre edilmiştir. Bu nedenle bu tür sistemlerin finansal raporlama işlemleri ile bağlantısı çok yüksektir. Söz konusu sistemlerin Sarbanes-Oxley Yasası ile uyumlu olup olmadığı değerlendirilmedir.[222]

Sarbanes-Oxley Yasası organizasyonlar için en efektif ve en uygun iç kontrol yapısının ve/veya çevresinin organizasyonlar tarafından seçilmesini ve uygulanmasını zorunlu tutar. COSO ise organizasyonlar tarafından seçilen ve uygulanan en uygun iç kontrol yapısı olarak karşımıza çıkmaktadır. Ancak COSO uygulaması; bilgi teknolojileri ile ilgili olan kontrollerin oluşturulması ve uygulanması konusunda organizasyonlar için en iyi uygulamaları ortaya koymamaktadır.

[222] Şirketlerin finansal raporlamaları üzerindeki kontrollerin iyileştirilmesini amaçlayan ve aynı zamanda etkin kurumsal yönetimi destekleyen bir çaba olarak görülen Halka Açık Şirketler Muhasebe Reformu ve Yatırımcıyı Koruma Yasası veya diğer adıyla Sarbanes-Oxley yasası, Amerika Birleşik Devletleri'ndeki borsalarda işlem gören halka açık şirketlerin tamamını kapsayacak şekilde 30 Temmuz 2002'de imzalanmıştır.

Bu sebeple COBIT standartları ile COSO küpü içerisinde yer alan bileşenler dikkate alındığında, bir işletme için uygulanması gereken ideal kontroller bütünü karşımıza çıkmaktadır. Yukarıda yer alan Tablo 3 içerisinde COBIT standart uygulamaları ile COSO küpü içerisinde yer alan bileşenlerin bağlantıları kurularak, COBIT standartlarının uygulanması durumunda söz konusu bu uygulama maddesinin hangi COSO küpü bileşenini karşıladığı gösterilmiştir.

3.6 Bankacılık Sektöründe Bilgi Sistemleri Denetimi İle İlgili Yasal Mevzuat

Bankacılık sektöründe faaliyet gösteren bankalara ait bilgi sistemlerinin denetlenmesinin amacı; 26170 sayılı "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" kapsamında açıklanmıştır. Yönetmelik; bankaların bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesiyle ilgili usul ve esasları düzenleme amacını taşımaktadır.[223]

İlgili yönetmelik kapsamında bankalarda gerçekleştirilecek bilgi sistemleri denetimi, uygulama kontrolleri denetimi ile genel kontrol alanları denetimini kapsadığı belirtilmiştir. Yayınlanan yönetmelik, banka bünyesinde yer alan uygulama kontrollerine ait denetim faaliyetinin senelik olarak, genel kontrol alanlarına yönelik denetim faaliyetlerinin iki sene de bir olarak bağımsız denetim kuruluşlarınca gerçekleştirilmesi gerektiğini zorunlu hale getirmiştir. Yönetmelik kapsamında ayrıca; bağımsız denetim kuruluşları tarafından gerçekleştirilen denetim faaliyetlerinin bankanın finansal tablolarında önemli etkileri bulunan iştirakleri ve/veya bağlı ortaklıkları da kapsaması gerektiği belirtilmiştir.

Denetim faaliyeti gerçekleştirilecek olan banka bünyesinde, banka tarafından gerçekleştirilen uygulama kontrol çeşitlerinden hangilerinin bilgi sistemleri denetim kapsamına dahil edilmesi gerektiği, kontrollerin yer aldığı süreçlerin "önemlilik" ve "risk" düzeyi değerlendirilerek belirlenmelidir. Belirlenen düzey bilgisi, denetim

[223] BDDK, "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" (Madde 1, Sayı 26170; Tarih: 16 Mayıs 2006), s.1.

içeriğinin ve kapsamının belirlenmesine yardımcı olur. Süreçlere ait "önemlilik" ve "risk" düzeyi denetim çalışmasını yönlendirerek, işin niteliğini ve kapsamını belirler. "Önemlilik" ve "risk" kavramları arasında farklılık bulunmakla birlikte; riske dayalı tespit edilen konuların, önemlilikle ilgili kararları farklı yönde etkilemesine izin verilmemesi gerekir. Risk kavramının hata ihtimali ile ilişkisi bulunmakla birlikte; önemlilik kavramı ise ortaya çıkan hata işleminin işletme tarafından ne dereceye kadar kabul edilebileceği temeline dayanır.[224]

Banka tarafından gerçekleştirilen faaliyetlerde yer alan uygulama kontrolleri denetlenirken, denetim kapsamında denetlenme faaliyeti yürütülecek olan sürecin bankadaki önemlilik düzeyleri değerlendirilerek kapsam belirlenir. Denetim faaliyeti yapılacak olan süreç üzerindeki kontroller test edilmektedir. Uygulama kontrolleri denetimi kapsamında değerlendirilecek bazı süreçler krediler, mevduat, menkul kıymetler, hazine operasyon vb. süreçlerden oluşmaktadır.

Banka bünyesinde yürütülen faaliyetlerde yer alan genel kontrol alanlarının da denetim faaliyetini yürüten bağımsız denetim firması tarafından belirlenmesi ve denetim kapsamının netleştirilmesi gereklidir. BDDK tarafından, 31 Aralık 2007 tarihi itibarıyla 16 Mayıs 2006 tarih 26170 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" kapsamındaki 14, 15, 16 ve 17. maddeleri içerisinde genel kontrol bölümlerinin ne şekilde denetlenmesi gerektiği ile ilgili olarak içerik ve kapsam belirlenmiştir. Yönetmelik içerisinde; genel kontrol alanlarının denetiminde ISACA isimli uluslararası kuruluşun oluşturduğu BT yönetişim standardı olan "Bilgi Teknolojilerine Yönelik Kontrol Hedefleri" ("COBIT") dokümanını kapsam olarak zorunlu kılmıştır. Bu kapsamda; yukarıdaki bölümlerde belirtilen COBIT genel kontrollerinin, denetim kapsamına alınmasını zorunlu kılmıştır.

BDDK tarafından, banka bünyesindeki uygulama ve genel kontrollerinin denetim faaliyetlerinin gerçekleştirilmesine ek olarak; 14.09.2007 tarihli ve 26643 sayılı

---

[224] Berna DİNÇ, "Mali Denetimde Önemlilik Kavramı", **Sayıştay Dergisi**, Sayı:50-51, Temmuz-Aralık 2003, s.142.

"Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler Tebliği" 1 Ocak 2008 tarihinde yürürlüğe girmiş olan tebliğin içeriğinde yer alan gerekliliklerinin bankalar tarafından uygulanıp uygulanmadığının kontrol edilmesi ve incelenmesi işlemini denetim faaliyeti kapsamına dahil etmiştir.

BDDK[225] tarafından 14.09.2007 tarihinde yayınlanan "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" kapsamında; sektör bünyesinde faaliyet gösteren bankaların, bankacılık operasyonlarında bilgi teknolojilerini kullanmasından kaynaklanan riskleri tanımlaması, analiz etmesi, izlemesi ve yönetilmesi açısından zorunlu olan tedbirleri alması gerektiği belirtilmiştir.[226]

Bilgi sistemleri ile ilişkili olan risklerin banka bünyesinde yönetilmesi kurumsal bilgi sistemleri yönetiminin önemli bir kısmını oluşturur. Banka bünyesinde üst yönetim tarafından oluşturulan risk yönetim politikaları oluşturulurken, bilgi teknolojileri kullanımına ilişkin risklerin ve kriterlerin dikkate alınması gereklidir. Bilgi teknolojilerinin kullanımına bağlı olarak oluşan riskler, bankacılık faaliyetlerinde belirlenen standart risk sınıflamalarında ek bir sınıf olarak yer almamaktadır. Bilgi teknolojilerine bağlı olarak oluşan risklerin yönetimi ve izlenmesi ile ilgili olan çalışmalarda temin edilen bilgiler, bankaya ait genel risk yönetim çerçevesi oluştururken dikkate alınmalıdır. Bilgi teknolojilerine ait oluşan risklerin, bankaya ait risk yönetim çerçevesi içerisinde birlikte yer alması sağlanarak, bütünleşik bir yönetim yaklaşımı oluşturulmalıdır. Banka yönetiminin belirlediği periyotlarda ve/veya bilgi teknolojilerinde meydana gelen değişikliklerden önce risk analizlerinin tekrarı sağlanmalı ve yapılan analizlerle ilgili olarak yazılı politikaların oluşturulması sağlanmalıdır.

Yayınlanan ilkeler tebliği üç ana bölümden oluşmakla birlikte; ilkeler tebliği kapsamında bankalardaki bilgi sistemlerine ilişkin risk yönetiminin ve iç kontrollerin oluşturulması konusunda uygulanması gereken işlemlere değinilmiştir.

---

225 BDDK: Bankacılık Düzenleme ve Denetleme Kurumu

226 BDDK, "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" Madde 5, Sayı: 26643, Tarih 16 Eylül 2007, s.3-4.

1) Bilgi Sistemlerine Yönelik Risk Yönetimi

2) Bilgi Sistemlerine Yönelik İç Kontrollerin Tesisi ve Takibi

3) İnternet Bankacılığı ve ATM gibi Önemlilik Arz Eden Bazı Konular Hakkında Hükümler

Ayrıca 1 Kasım 2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik" genel kontrol alanlarının denetimi kapsamında uluslararası bir kuruluş olan Bilgi Teknolojileri Yönetimi Enstitüsü tarafından yayınlanan "COBIT" dokümanını standart olarak kabul etmiştir.

COBIT ("Control Objectives for Information and related Technology") genel olarak kurumların bilgi teknolojileri yönetişim alanında gelişme kaydetmesindeki amaçları ve yolları gösteren, kurumların bilgi teknolojileri yönetişim alanında kendilerini değerlendirmeyi sağlayan yol gösterici bir uygulamadır. Bu nedenle COBIT'in detay açıklamalarına girmeden önce, ulaşmayı hedeflediği etkin bilgi teknolojileri yönetişimin tanımını yapmak gereklidir.[227]

Bilgi teknolojileri yönetişimi ("IT Governance"), üst yönetimin sorumluluğundadır. Bilgi teknolojileri yönetişimi; liderlik, organizasyonel yapı, kurumun stratejilerinin ve hedeflerinin genişletilmesinde ve desteklenmesinde bilgi teknolojileri fonksiyonundan stratejik olarak faydanılmasını sağlayan yönetim biçimi ya da anlayışıdır. COBIT uygulaması bu bakımdan uzman kişilerin fikir birliğine vardığı ve bilgi teknolojileri yönetişimin etkin olarak sağlanmasında destek olacak en iyi örnekleri, yönetilebilir ve mantıksal bir çerçevede sunmayı hedefleyen yol gösterici bir uygulamadır.[228]

Bankalar; yapılacak olan bilgi sistemleri denetimi kapsamında; yönetmelikte belirlenen yükümlülüklerini yerine getirmesi gereklidir. Bankaların bilgi sistemleri ve

---

[227] Robert LAWTON, "Transitioning IT From a Compliance to a Value-Driven Enterprise Using CobiT", **Information Systems Control Journal**, volume:6, 2007, s.43.

[228] ISACA COBIT, a.g.e., s.5.

bilgi sistemleri ile ilgili oluşturulmuş olan doküman; finansal veri üretim prosesleri ile ilgili belge, bilgi, kayıt ve uygulama; bilgi sistemleri yapısında bulunan bütün genel ve uygulama kontrollerinin oluşturulması, denetlenen bankaların sorumluluğu kapsamındadır. İlgili genel ve uygulama kontrollerinin oluşturulmasının yanında, etkili ve verimli bir şekilde kontrollerin uygulanması ve faaliyetlere uygun ve asgari ölçüde bir kontrol ortamının oluşturulmasına yönelik işlemler de denetlenen bankaların sorumluluğu kapsamındadır. [229]

Bankalar, gerçekleştirdikleri işlemlerle ilgili olarak uygulama listesi oluşturur. Uygulama listesi içerisinde operasyonel ve finansal faaliyetlerini, mevcut durumda kullanmış oldukları tüm sistem, uygulama ve kullanım amaçlarını içermektedir. Banka tarafından oluşturulan uygulama listesinin denetim faaliyetini gerçekleştiren denetim ekibine bildirilmesi gereklidir. Örneğin operasyonel olarak krediler; mevduat, swıft işlemlerini gerçekleştirdiği tüm sistemlerin niteliklerini, kullanım alanları bazında denetçiye bildirmek zorundadır.

Banka bünyesinde yürütülen faaliyetlere ait finansal verilerin oluşturulduğu süreçler ve finansal verileri oluşturan tüm önemli ve kritik sistemlerin ve uygulamalara ait kontroller banka bünyesinde denetim çalışması öncesinde belirlenmeli, değerlendirilmeli ve takip edilmesi gereklidir. Uygulama kontrolleri değerlendirilirken, aşağıdaki kriterler dikkate alınmalıdır:

1. Banka bünyesinde yer alan sistemlerin yazılı olarak oluşturulan dokümantasyonlarla uyumu,

2. Yazılı kontrollerin yeterliliği ve banka bünyesinde uygulanma derecesi,

3. Kullanılan sistemlerin bünyesinde yer alan ve/veya oluşturulan verilerin güvenliği, bütünlüğü ve sürekliliği değerlendirilmelidir.

[229] BDDK, "Bankalarda Bilgi Sistemleri Yönetmeliğinde Esas Alınacak İlkelere İlişkin Tebliğ", Madde:22, Sayı:26643; Tarih:16 Eylül 2007, s.14.

"Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" kapsamında, COBIT uygulamaları dikkate alınarak; banka içerisinde uygulanan uygulama kontrollerinin yanında genel kontrol konusu yer alan süreçler için, süreç bazında aşağıdaki belirtilen hususlara uygun bir koşulun yerine getirilmesinden ve tesis edilmesinden banka yönetimi sorumludur.[230]

1. Süreç Sahibi: Banka bünyesinde süreç kapsamında uygulanan her bir genel kontrol için süreç sorumlu belirlenir. Belirlenen sorumlu kişiye ait sorumluluklar tam, doğru ve açık bir şekilde tanımlanır.

2. Tekrarlanabilirlik: İş süreçleri içerisinde yer alan genel kontrol konuları, tekrarlanabilir özellikte olacak şekilde belirlenir ve tanımlanır.

3. Hedefler ve Amaçlar: Genel kontrollere sahip olan süreçler için tam, doğru ve net bir şekilde tanımlanmış hedefler ve amaçlar oluşturulur. Hedef ve amaçlar genel kontrollerin etkin ve verimli bir şekilde tanımlanması için oluşturulur.

4. Roller ve Sorumluluklar: Banka bünyesinde tanımlanan kontrollerin etkin ve verimli bir şekilde işlemesi amacıyla, roller, faaliyetler ve sorumlulukların sağlanması ve gerekli olan tanımlamaların yapılması sağlanır.

5. Süreç Performansı: Bankanın belirlemiş olduğu hedefler kapsamında, ilerleyen ve yenilenen süreç kapsamında gerekli olan geliştirmelerin yapılabilmesi amacıyla genel kontrollere ait süreçlerin performansları ölçülür.

6. Politikalar, Planlar ve Prosedürler: Banka bünyesinde oluşturulan genel kontrollerle ilgili olarak politikalar, planlar ve prosedürler yazılı hale getirilir. Yazılı hale getirilen dokümanlar, banka bünyesinde belirlenmiş olan periyotlar dahilinde kontrol edilerek revize edilir. Revize edilen dokümanlar yönetim tarafından kontrol edilir ve onaylanır. Yönetim tarafından onaylanan dokümanlar ilgili bölümlerle paylaşılır.[231]

---

230 BDDK, "Bankalarda Bilgi Sistemleri Yönetmeliğinde Esas Alınacak İlkelere İlişkin Tebliğ", Madde:22, Sayı:26643, Tarih:16 Eylül 2007, s.14.

231 BDDK, "Bankalarda Bilgi Sistemleri Yönetmeliğinde Esas Alınacak İlkelere İlişkin Tebliğ", Madde:22, Sayı:26643, Tarih:16 Eylül 2007, s.14.

4. BÖLÜM
BANKALARDA KREDİLENDİRME SÜRECİ ve KREDİ SÜRECİNDE YER ALAN RİSK ÇEŞİTLERİNİN ÖNLENMESİ

Bankacılık sektöründe aşağıdaki belirtilmiş olan temel süreçler kapsamında bankalar operasyonlarını yürütmektedir. Söz konusu süreçler banka bünyesinde belirlenen stratejilere göre güncellenebilir, belirtilen süreçlere ait kontrol faaliyetlerinin banka bünyesinde tam, doğru ve zamanında gerçekleştirilmesi gereklidir. Süreçler ve süreçlere ait uygulanan kontrol işlemleri süreç bazında aşağıdaki gibidir:[232]

a) Mevduat Süreci: Müşteri mevduat hesapları ile ilgili olarak gerçekleştirilen işlemler, çek/senet, fon transferi ve tahsilat işlemleri, mevduatın sınıflandırılması, tasarruf mevduatı kapsamının belirlenmesi ve tasarruf mevduatı sigorta primlerinin hesaplanması gibi hesaplama kontrolleri, kara para aklanmasına ilişkin kontroller, işlemlerin muhasebeleştirilmesi ve süreç içerisindeki diğer kontrolleri,

b) Bireysel/Kurumsal Kredi Süreçleri: Kredi başvurularının alınması, değerlendirilmesi, kredi tahsisi ve kullandırımı işlemleri ve onayları, teminatlandırma, kredi limitleri ile kredi geri ödeme tabloları ve hesaplamalarına ilişkin kontroller, takip hesaplarına aktarım süreci ve karşılık hesaplamaları, kredilerin sınıflandırılması, yaşlandırma raporlarının hazırlanması ve yeniden yapılandırma işlemleri, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri,

c) Muhasebe Süreci: Faiz, gelir/gider tahakkuku ve reeskont hesaplamaları, işlem bazında tek düzen hesap planına uygunluk, amortisman hesaplamaları, muhasebe fişi oluşturulmasına ait yetkilendirme süreci, mizanın oluşumu, geriye dönük muhasebe fişi kesilmesi işlemleriyle ilgili yetkilendirmelerin varlığı ve ilgili kayıtların bütünlüğü ve izlenebilirliği, işlem numaralarının ardışıklığının sağlanması, işlem limitlerinin ve

[232] BDDK, "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik", Madde 25, Sayı 27461, Tarih: 13 Ocak 2010, s.12-13.

yetkilerinin kontrolü, şube ve genel müdürlük kayıtları arasındaki mutabakat işlemleri, hesap planı düzenleme ve değişikliklerine ilişkin kontroller, defteri kebir hesapları ile yardımcı, alt ve geçici hesapların mutabakatı, yasal ve yardımcı defterler arası mutabakatlar, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri,

d) Alternatif Dağıtım Kanalları Süreci: Elektronik bankacılık/alternatif dağıtım kanalları ile ilgili yetkilendirme, kimlik doğrulama, muhasebeleştirme ve diğer süreç kontrolleri,

e) Banka ve Kredi Kartları Süreci: Banka ve kredi kartı başvuru değerlendirme, limit tahsisi, kart basım ve dağıtım işlemleri, üye işyeri ve POS işlemleri, kartların kullanımı ve hediye puanı gibi uygulamalara ilişkin kontroller, takip hesaplarına aktarım süreci ve karşılık hesaplamaları, yaşlandırma raporlarının hazırlanması ve yeniden yapılandırma işlemleri, banka ile kart merkezi mutabakatları gibi mutabakat kontrolleri, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri,

f) Finansal Raporlama Süreci: Banka kayıtlarının ve bilgi kaynaklarının finansal raporlamalarda kullanım sürecinin kontrolü ve diğer süreç kontrolleri,

g) Ödeme Sistemleri Süreci: EFT, EMKT, Takasbank, SWIFT işlemleri ve bu işlemlere ait güvenlik kayıtları gibi ödeme sistemi kontrolleri, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri,

h) Hazine/Menkul Kıymetler ve Fon Yönetimi Süreci: Menkul kıymet ve fon yönetimi iş süreçlerinin kontrolü, türev ürünleri, nostro, vostro ve loro bakiyelere ilişkin mutabakatlar ve muhabir kayıtlarının kontrolü, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrollerini içermektedir.

Yukarıdaki belirtilen süreçlere ait risklerin etkin ve verimli bir şekilde yürütülmesi, söz konusu süreçlerde yer alan kontrollerin tam ve doğru bir şekilde belirlenmesine bağlıdır. Süreçler içerisinde yer alan kontrollerin doğru tanımlanmasının yanında söz konusu kontrollerin periyodik olarak test edilmesi gereklidir.

Banka bünyesinde yer alan süreçler değerlendirildiğinde, kredi süreçleri içerisindeki operasyonel faaliyetlerin sonuçları bankalar için büyük önem arz etmektedir.

4.1 Bankacılık Sektöründe Kredi ve Kredi Riski Kavramı

Gelişen teknolojiye bağlı olarak bankacılığın gün geçtikçe uluslararası nitelik kazanması, sunulan finansal hizmetlerin de çeşitlilik kazanmasına ve bu nedenle bankalar tarafından sağlanan hizmetlerin yeniden tanımlanmasına neden olmuştur. Bankalar bünyesinde yürütülen bankacılık faaliyetlerinden en risklisi ve önemlisi kredilendirme sürecinde gerçekleştirilen işlemlerdir. Kredi faaliyetlerine ait sürecin tam ve doğru bir şekilde anlaşılabilmesi açısından kredi tanımı, unsurları ve fonksiyonlarının anlaşılması ve banka tarafından belirlenen strateji ve hedeflere uygun olarak kredilendirme süreci kapsamında dikkat edilmesi gereken işlemlerin belirlenmesi gereklidir.

Kredilendirme faaliyeti, kredi talebinde bulunan ve/veya banka tarafından kredilendirilmek istenen müşteriyle ilk iletişime geçilmesiyle başlar. Bu süreç daha sonra, krediyle bağlantılı olan anapara, faiz, komisyon vb. değerlerin ödemelerinin yapılması ile devam eder. Kredilendirme faaliyeti, yapılan ödemelerden sonra müşteriden alınan teminat bedellerinin çözülmesi ile sonlanmaktadır. Söz konusu süreç içerisinde geçen zaman dilimi arasında gerçekleştirilen bütün işlemler kredilendirme işlemini ifade eder.[233] Banka merkezi dışında gerçekleştirilen kredilendirme işlemlerinin temel adımları ve görev alanlarında yapılması gereken temel ve alt işlemler regülasyon tarafından belirlenmiştir.

4.1.1 Kredi Tanımı, Unsurları ve Fonksiyonları

Kredi sözcüğü; Lâtince‟de "Creditum – Credere" kelimelerinden meydana gelmektedir. Kredi kelimesi dilimizde, itimat etmek, inanmak anlamına gelen, "itibar, güven" olarak ifade edilmektedir.

Sözlük anlamı açısından incelendiğinde kredi; ödünç verilen tutar, belirli bir süre sonra geri almak kaydı ile bir satın alma gücünün sağlanması veya var olan satın alma

[233] Yıldız AYANOĞLU ve Burak ERTÜRK, "Modern Kredi Riski Yönetiminde Derecelendirmenin Yeri ve İMKB'ye Kayıtlı Şirketler Üzerinde Bir Uygulama**", Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Sayı:9, Şubat 2007, s.77.

gücünün başka bir kişiye devredilmesi ya da bir kişi veya kurum lehine kefil olunması; kabul, aval, garanti verme işlemidir.[234]

Bankacılık faaliyetleri ile ilgili olarak bir tanım yapılması gerekirse; bankanın gerçek veya tüzel kişilere yasalar, iç politikaları ve kendi kaynakları kapsamında, teminat karşılığı ve teminatsız olarak para, teminat veya kefalet vermek şeklinde tanınmış olan olanak ve limitler olarak tanımlanabilir. Söz konusu bu işlem gerçekleştirilirken banka tarafından araştırma ve/veya istihbarat sonuçlarının dikkate alınması durumu öncelikli ve temel bir kriter olarak sağlanır.[235]

Bankacılık Kanunu'nun 48.maddesine göre kredi tanımı "Bankalarca verilen nakdi krediler ile teminat mektupları, kontrgarantiler, kefaletler, aval, ciro, kabul gibi gayri nakdi krediler ve bu niteliği haiz taahhütler, satın alınan tahvil ve benzeri sermaye piyasası araçları, tevdiatta bulunmak suretiyle ya da herhangi bir şekil ve surette verilen ödünçler, varlıkların vadeli satışından doğan alacaklar, vadesi geçmiş nakdi krediler, tahakkuk etmekle birlikte tahsil edilmemiş faizler, gayri nakdi kredilerin nakde tahvil olan bedelleri, ters repo işlemlerinden alacaklar, vadeli işlem ve opsiyon sözleşmeleri ile benzeri diğer sözleşmeler nedeniyle üstlenilen riskler, ortaklık payları ve kurulca kredi olarak kabul edilen işlemler izlendikleri hesaba bakılmaksızın bu kanun uygulamasında kredi sayılır." şeklinde yapılmıştır.[236]

Krediye ait birden fazla yapılan tanıma göre kredi tanımı içerisinde 4 ana unsur bulunmaktadır. Bu kavramlar sırasıyla **zaman (vade), itimat (güven) risk ve gelir** kavramlarından oluşmaktadır.[237]

---

[234] Kürşat ÖZGÜR ÖZDEN, "Ticari Bankalarda Kredilendirme Süreci ve Kredi Riski Yönetimi", **Yüksek Lisans Tezi**, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2010, s.3.

[235] Kaan BALKAŞ, "Kredi Kavramı ve Sektör Kredilerine Göre Türkiye'deki Belli Başlı Sektörlerin Analizi", **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2004, s.4.

[236] BDDK, "5411 Sayılı Bankacılık Kanunu", Sayı: 25983, Tarih:1 Kasım 2005.

[237] Can TANSEL TUĞCU ve Ekrem ERDEM, **Bankalarda Kredi Yönetimi**, Anadolu Üniversitesi, 1.Baskı, Eskişehir, Haziran 2012, s.17.

Zaman (Vade): Karşı tarafa ödünç olarak, borç olarak verilen paranın belirlenen belli bir süre sonrasında iade edilmesi koşulu yer aldığından zaman (vade) kavramı ortaya çıkar. Zaman (vade) süresinin artmasına bağlı olarak risk faktöründe artış ortaya çıkar, bunun nedeni, geleceğe bağlı olarak belirsizliğin artmasından kaynaklanmaktadır.[238]

Güven: Karşı tarafa verilen ve/veya sağlanan kredi miktarının belirlenen süre sonunda geri ödenmesi koşulu taşımaktadır. Bu koşul nedeniyle güven unsurunun süreç kapsamında yer alması gereklidir. Kredi verilecek ve/veya sağlanacak olan müşterinin faaliyet gösterdiği sektör içerisinde belirli bir saygınlığı bulunması gereklidir. Kredi işlemleri içerisinde önemli bir kriter olarak ortaya çıkan güven ve saygınlık, nakit, mal, teminat, kefalet biçiminde veya herhangi bir şekilde verilen kredi, belirli bir süre sonunda geri alınmak koşulunu taşıdığından, güven unsurunun mutlak suretle oluşması sağlanmalıdır. Özetlemek gerekirsek; kredi kavramı içerisinde zaman unsurunun yer alması, güven kavramının en temel yapı taşıdır.[239] Kredi kullandıran ile krediyi kullanan arasında oluşan ilişki, temel olarak güven unsuru üzerinde oluşur ve gelişir. Güvenin sağlanması amacıyla; kredi kullandırma yetkisini elinde bulunduran finansal kuruluşlar, kredi kullanma talebinde bulunan müşterilerin, sahip olduğu bilgileri incelemekte ve yaptıkları inceleme ve değerlendirmelere göre kredi sürecinin oluşmasını sağlamaktadır. Bu kapsamda kredi kullandıran ve/veya sağlayan kuruluşlar, belirli durumlarda müşteriden kefalet ve/veya teminatlar alarak, güven kavramının temelinin oluşmasını sağlar.[240]

Risk: Risk tanımı, müşteriye ödünç olarak verilen tutarın tahsiline ve verilen garantiye konu yükümlülüğün sağlanmasına kadar ortaya çıkması beklenen muhtemel tehlikelerin toplamını ifade eder.[241] Kredi riski, kredi müşterisinin krediyi tahsis eden tarafa kredi ilişkisine istinaden oluşturulan kurallara aykırı davranması durumunda, krediyi kullandıran taraf arasında yapılan sözleşme maddelerine uygun davranmamasını

---

238 Dilek ARSLAN, "Bankacılık Sektöründe Kredi Kullanıcılarının Değerlendirilmesi", **Yüksek Lisans Tezi**, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2014, s.28.

239 ARSLAN, a.g.e., s.28.

240 TUĞCU ve EKREM, a.g.e., s.17.

241 ARSLAN, a.g.e., s.28.

ifade eder. Kredi riski, kredi müşterisinin aldığı kredi miktarını anlaşılan ve/veya sözleşme içerisinde belirtilen süre içerisinde geri ödememesi ya da eksik ödeme yapması durumunda kredi kullandıran tarafından karşılaşacağı maddi kayıp miktarını ifade eder.[242]

Gelir: Kredi kullandıran tarafların temel amacı, gerçekleştirilen faaliyet kapsamında bir gelir sağlamaktır. Kredi kullandıran tarafından stratejik hedefine bağlı olarak, kredi kullanan taraftan elde edilen gelirin belirli bir miktarı kullandırılan kredi tutarına kaynak oluşturan mevduat sahiplerine gelir olarak verilir. Kalan kısım ise kredi kullandıran tarafa ait kar miktarını oluşturur. Kredi kullandıran tarafından kredi kullandırım işleminden elde etmiş olduğu kar miktarının artması, kredi kullandıran diğer tarafların etkinliğinin artmasına olanak sağlar. Kredi kullandırımından elde edilen gelir miktarının büyüklüğü kredi kullandıran tarafların faaliyet gösterdiği piyasaların daha etkin ve verimli bir şekilde işlem görmesini sağlar.[243]

Bankaların temel olarak gerçekleştirdiği işlemler, kaydi para yaratma, sermaye piyasasında aracılık faaliyetlerinde bulunma, müşteri temelli hizmet ağı faaliyetlerinden oluşmaktadır. Kredilendirme işlemleri yürütülen bu işlemlerin en önemlisidir. Bunun nedeni bankacılık sektöründe kredi veren kuruluşlar tarafından gerçekleştirilen kredilendirme fonksiyonu, ülke ekonomisinin canlanmasına neden olmakta; işletmelerin riski yüksek yatırımlarında riskin paylaşılmasını sağlayarak işletmelerin büyümelerine katkı sağlamaktadır. Bankalar ve diğer finans kuruluşları tarafından gerçekleştirilen kredilendirme faaliyetlerinin etkinliği, faaliyet göstermiş oldukları ekonomideki finansal durgunluğun kaybolmasına neden olmakla birlikte, ilgili ekonomi içerisindeki girişimcilerin daha fazla rol aldığı bir faaliyet ortamının oluşmasına olanak sağlayacaktır.[244]

---

[242] Hüseyin SELİMLER, "Sorunlu Kredilerin Analizi, Banka Finansal Tablo Oranlarına Etkisinin Değerlendirilmesi", **Finansal Araştırmalar ve Çalışmalar Dergisi**, Cilt:7, Sayı:12, Ocak 2015, s.137.

[243] TUĞCU ve EKREM, a.g.e., s.18.

[244] Ezgi YILDIRIM, "Bankalarda Ticari Kredilendirme Süreci; Karşılaşılan Sorunlar ve Çözüm Yolları İle İlgili Ampirik Bir Çalışma", **Yüksek Lisans Tezi**, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2007, s.5.

4.1.2 Kredi Riski Tanımı ve Kredi Riski Çeşitleri

Kredi riski, bankaların taşıdığı risklerden en önemlisi olarak adlandırılabilir. Kredi kullandırım miktarının kısmen veya tamamen geri alınamaması durumunun oluşma ihtimalini ifade eder.[245]

Banka bünyesinde kredi faaliyetlerini yürütürken dikkate alınması gereken hususlar önceden belirlenmiş ve uygulanabilir hale getirilmiştir. Kredi işlemleri ile ilgili olarak belirlenen kriterler ve uygulama şekilleri dışında banka bünyesinde kredi riskinin kaynağı ve oluşması itibariyle kredi riskinin aşağıdaki yer alan başlıklar kapsamında değerlendirilmesi gereklidir:[246]

a) Kredi İşleminin Sonuçlandırılamama Riski: Bankanın kredi kullandırdığı taraftan belirlenen ve/veya hedeflenen tarihte kullandırmış olduğu kredi miktarını geri alamaması durumunu ifade eder. Bu durum, kredi miktarının zamanında ve/veya tam olarak karşı taraftan temin edilememesi sonucunda ortaya çıkabilir. Kredi kullandırılan tarafla ilgili olan en temel kredi riski olarak bu risk oluşabilir.

b) Konsantrasyon (odaklanma) Riski: Kredi kullandırım işlemi kapsamında grup, sektör, coğrafi yapı gibi bilgi ve sınıflandırmalara dikkat edilmemesi ve bunun sonucu olarak yüksek montanlı olan kredilerin az sayıda müşteri kitlesine kullandırılmasına istinaden oluşan risk türünü ifade eder. Söz konusu risk durumunun oluşmaması amacıyla bankalar tarafından yıllık ve ara dönemlerde faaliyet raporları hazırlanır. Faaliyet raporları kapsamında, kullandırmış oldukları kredilerini, sektörel ve risk grupları bazında periyodik olarak değerlendirirler.

c) Ülke Riski (Hâkimiyet Riski ve Transfer Riski): Kredi kullandırma işleminin uluslararası piyasalarda gerçekleştirilmesi durumunda; kredi kullandırılacak

---

[245] Oya GÜVERCİNCİ, "Bankalarda Risk Yönetimi",15.03.2011, http://www.riskonomi.com/wp/?p=392, (15.03.2011), s.2.

[246] Aslı YÜKSEL MERMOD ve Mustafa CERAN, "Basel III Doğrultusunda Bankacılık Riskleri ve Sermaye Yeterliliği; Türk Bankacılık Sektörü Üzerine Karşılaştırmalı Bir Analiz", **Finansal Araştırmalar ve Çalışmalar Dergisi**, Cilt:2, Sayı:4, 2011, s.32.

olan müşterinin faaliyet gösterdiği ülke içerisindeki sosyal, ekonomik, politik yapı nedeniyle oluşabilecek olan risk türünü ifade eder. Ülke riski kapsamında, kredi kullandırımının yapılacağı müşterinin faaliyet gösterdiği ülke yönetimine ait hâkimiyet riski ve/veya kullandırılacak olan kredi miktarına ait para transferlerine ait yaşanabilecek olan riskler yer alır.

d) Karşı Karşıya Kalınan Risk: Kredi kullandırım işlemi sonucunda, kredi kullandıran finansal kuruluşun katlandığı toplam risk miktarı, ana kredi ve kredinin biriken faiz bedelinden oluşmaktadır. Bu nedenle, krediyi kullandıran taraf toplam risk kapsamında değerlendirme yaparken, verilen kredi miktarını değil, verilen kredi miktarının sağladığı kar olan kredi faizlerini ya da kar paylarını dikkate alır.

e) Tazmin Edememe Riski: Kredi kullanımı yapan tarafından kredi ile ilgili olarak yükümlülüklerini yerine getirememesi, kredi kullandırımı yapan tarafın kredinin karşılığı olan miktarı kredi kullanan taraftan temin edememesi durumunda, kredi kullandıran tarafın temin etmiş olduğu teminatları değerlendirme yeteneğine bağlı olarak tanımlanan risk türünü ifade eder. Kredi işlemlerine ait süreç kapsamında teminat bilgisi güçlü olan müşterilere ait bazı sakıncalar göz ardı edilerek kredi tahsisi yapılmaktadır. Bu durum hatalı bir uygulama olmakla birlikte; bazı teminat bedellerinin nakde çevrilmesine ilişkin oluşabilecek zorluklar ve aksaklıklar dikkate alınmamaktadır. (örn. Teminat bedelinin nakde dönüştürülmesi sürecinin zaman alması, alınan teminat miktarının kredi miktarını karşılamaması vb.) Kredi kullandırım işlemlerinde alınan teminatın çeşidi ve miktarı önemli olmakla birlikte, teminat çeşidine ve miktarına göre müşterilere verilecek olan kredi miktarının belirlenmesi hatalı bir yaklaşım tarzı olarak karşımıza çıkar.

f) Kredi İşleminin Sonuçlandırılması Öncesi Oluşan Risk: Kredi kullandırımı yapan tarafın, kredi kullanan müşterisine ait sözleşme içerisinde belirtilen sorumluluk ve yükümlülüklerini tamamlayamayacak olmasının önceden tespit edilmesi durumuna bağlı olarak oluşan risk türünü ifade eder. Bu durum oluştuğunda, kredi kullandırımı yapan taraf, kredi miktarının geri ödenmesi için daha önceden aksiyon alma kriterlerinin oluşturulmasını sağlamalıdır.

Kredi riskinin bankacılık sektöründe en önemli riskler arasında yer alması ile beraber, söz konusu sürece ait operasyonel faaliyetlerin gözetimi, değerlendirilmesi ve denetim işlemlerinin önemini arttırmıştır.

4.1.3 Kredi Türleri

Bankacılık sektöründe kullanılan kredi türleri 5411 sayılı bankalar kanununda tanımlanmıştır. 5411 Sayılı Bankalar Kanunu 48. maddeye göre aşağıdaki işlemler izlendikleri hesaba bakılmaksızın kredi niteliğinde işlem görürler[247]:

1. Bankalarca verilen nakdi krediler,

2. Teminat mektupları, kontrgarantiler, kefaletler, aval, ciro, kabul gibi gayrinakdî krediler ve bu niteliği haiz taahhütler,

3. Satın alınan tahvil ve benzeri sermaye piyasası araçları,

4. Tevdiatta bulunmak suretiyle ya da herhangi bir şekil ve surette verilen ödünçler,

5. Varlıkların vadeli satışından doğan alacaklar,

6. Vadesi geçmiş nakdî krediler, tahakkuk etmekle birlikte tahsil edilmemiş faizler, gayri nakdi kredilerin nakde tahvil olan bedelleri,

7. Ters repo işlemlerinden alacaklar,

8. Vadeli işlem ve opsiyon sözleşmeleri ile benzeri diğer sözleşmeler nedeniyle üstlenilen riskler,

9. Ortaklık payları,

10. Kurulca kredi olarak kabul edilen diğer işlemler,

[247] BDDK, "5411 Sayılı Bankacılık Kanunu", Sayı:25983, Tarih: 1 Kasım 2005.

11. Kalkınma ve yatırım bankalarının finansal kiralama yöntemiyle sağladığı finansmanlar,

12. Katılım bankalarının taşınır ve taşınmaz mal ve hizmet bedellerinin ödenmesi suretiyle veya kâr ve zarar ortaklığı yatırımları, taşınmaz, ekipman veya emtia temini veya finansal kiralama, mal karşılığı vesaikin finansmanı, ortak yatırımlar veya benzer yöntemlerle sağladıkları finansmanlar,

Yukarıdaki belirtilen işlemler dikkate alındığında krediler, çeşitli niteliklerde, çeşitli vade sürelerinde ve kullanım amaçlarına yönelik olarak birden fazla kredi türü uygulanmaktadır.

4.1.3.1 Kullanım Amaçlarına Göre Kredi Türleri

Kullanım amaçlarına göre krediler üretim ve tüketim kredileri olmak üzere 2 çeşittir.

1) Üretim Kredileri: Üretim kredileri, bir üretim biriminin faaliyete geçirilmesi ve üretim devamlılığının sağlanmasına yönelik olarak kullandırılan kredi türüdür. Üretim kredileri yatırım ve işletme kredisi iki çeşittir. Aşağıdaki tanımlamalar içerisinde kredi çeşitlerine ait detaylı tanımlama yapılmıştır.

a. Yatırım Kredileri: İşletmelerin faaliyetlerini gerçekleştirecekleri bina ve tesislerinin yapımı ve/veya kapasite arttırılması amacıyla (sabit kıymetlerin finansmanında kullanılmak üzere) açılan, süre olarak orta ve uzun vadeli kredileri ifade eder. Bu kredilere örnek olarak; fabrika, imalathane, yol, köprü, baraj, turistik tesisler vb. yapımı için kullandırılan krediler verilebilir. Genel olarak yatırım kredileri yatırım yapan işletme faaliyete başladıktan sonra kâr ettikten sonra geri ödenir. Bu nedenle yatırım kredileri genel olarak uzun vadeli krediler olarak tanımlanabilir.

b. İşletme Kredisi: Yatırım işlemleri tamamlanmış olan bir işletmeye ait üretim süreci için hammadde, malzeme temini ve işçilik ücretlerinin ödenmesi gibi üretilen ürünün satış aşamasına kadar olan finansman ihtiyacını karşılamak üzere açılan kredileri ifade eder. Kredinin vadesi, işletmeye ait hammaddenin satın alınma sürecinden,

üretilen ürünün faaliyet gösterilen sektör içerisinde müşteriye ulaştırılmasına kadar olan sürenin büyüklüğüne göre kısa ve orta vadeli olabilir.[248]

2) Tüketim Kredileri: Kredi kullanımı yapacak olan müşterinin, ilerleyen dönemlerde elde edeceği tasarruf miktarından karşılanması amacıyla ilgili müşterinin tüketim ürünlerini almalarını sağlayacak olan kredileri ifade eder. Söz konusu bu kredi türü tüketicilerin ihtiyaç duydukları ürünleri pazarlayan işletmeler, bankalar ve/veya diğer finans kuruluşları tarafından tüketicilerin hizmetine sunulur. Tüketici kredileri, ticari faaliyet dışında tüzel kişi nitelikte olmayan kişilerin mal ve hizmet alımları için ihtiyaç duyulan fon miktarının temin edilmesine yönelik olarak, kredilendirme aşamasının başlangıcında belirlenen faiz oranlarına göre bir seferde kullandırılan kredileri ifade eder.[249] Tüketici kredileri genellikle otomobil, dayanıklı tüketim maddeleri (beyaz eşya), ev eşyası, düğün-çeyiz, mesleki kuruluş, konut ve benzeri harcamalarda kullanılmaktadır. Kredi koşulları kredi kullandıran taraflarca farklılaşabilir.[250]

4.1.3.2 Teminatına Göre Kredi Türleri

1) Açık Kredi: Açık kredi, kredi kullanan müşteriden hiçbir tazminat bedeli temin edilmeden, müşteriye yönelik olarak yapılan kredi değerliliğine güvenilerek müşteri imzasına istinaden kullandırılan kredi türünü ifade eder. Açık kredi çeşidinin takibi borçlu cari hesap şeklinde yapılır. Bankalar, bu krediyi işletmelere; ihracat, hazırlık, akreditif teminatı ve kasa kolaylığı biçiminde kullandırmaktadır. Açık kredi türünde yasal otorite tarafından belirlenmiş herhangi bir yasal karşılık uygulaması bulunmadığından, diğer kredi türlerine göre daha risklidir. Kredi türüne ait riskin yüksek olması, kredilere ait kullandırım faiz oranının diğer kredilere uygulanan faiz oranından daha yüksek olmasına neden olmaktadır. Açık kredi kullandırımlarında kredi bedelinin, belirlenmiş vade süresinden önce ödenmesi talep edilebilir. Bu durum, kredi alan müşteri ile ilgili olarak yapılan değerlendirmenin sonuçlarının olumsuz yönde olması durumunda

---

[248] Songül YILMAZ, "Ticari Bankalarda Kredi Portföyü ve Kredi Riski Yönetimi-Bankacılık Sektöründe Bir Uygulama", **Yüksek Lisans Tezi**, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2010, s.16.

[249] YILMAZ, a.g.e., s.16

[250] A.Sait YÜKSEL, Aslı YÜKSEL ve Ülkü YÜKSEL, **Bankacılık Hukuku ve İşletmesi**, Beta Yayınları, 10.Bası, İstanbul 2004, s.556.

ortaya çıkar. Bu durumun oluşabilme ihtimaline bağlı olarak, bu çeşit krediler devamlı kullanılan krediler olarak nitelendirilmeyip, yardımcı nitelikte kullandırılan krediler olarak tanımlanabilir. Bu çeşit kredilere ait teminat karşılığı gösterme zorunluluğu bulunmamaktadır. Bu özellik nedeniyle bu çeşit kredilere ait kredi maliyetleri düşük oluşmaktadır. Kredi maliyetinin düşük olması, piyasada itibar sağlaması ve krediyi her an kullanabilme imkânının bulunmasını sağlar. Bu tür avantajlar bu kredi çeşidinin işletmeler tarafından tercih edilmesine neden olur.[251]

2) Teminatlı krediler: Kredi kullanımı yapan borçlunun borcunu ödemediği durumda kredi borcunun kredi kullanımı yapan kişiye kefil olan kişi ve/veya kurumun kabul ettiği kredileri ifade eder. Maddi teminat karşılığı kredi, bu krediler için teminat olarak mal, gayrimenkul ipoteği, işletme rehini, nakit, kıymetli madenler ve taşlar, hisse senedi ve tahvil vb. gibi maddi bir teminat alınabilir.[252]

3) Teminat Mektupları: Kredi kullandırımı sırasında kredi alan taraftan kredi kullandırımı yapan alacaklıya karşı olan borç yükümlülüğünün garanti edilmesi amacıyla, banka tarafından kredi alan tarafa verilen mektup türü teminat mektubu olarak ifade edilir. Teminat mektubu, kredi alan tarafın kredi borcu ile ilgili olarak yapmış olduğu sözleşme kapsamında yer alan yükümlülüklerini tam, doğru ve zamanında yerine getirmemesi durumunda, kredi kullandıran tarafın borç miktarını talep etmesi durumunda herhangi bir ön koşul ve kriter olmadan teminat mektubunda yazılı olan tutarı alacaklıya ödemeyi garanti etmektedir.[253] Teminat mektupları çeşit olarak hazırlanış şekillerine, süre ve limit bilgilerine göre sınıflandırılmaktadır.

4.1.3.3 Vade Bilgisine Göre Kredi Türleri

1) Vadesiz ve kısa vadeli krediler: Kullandırılan kredi miktarının alacaklı olan tarafa geri ödenmesi için herhangi bir zaman periyodu belirlenmeyen veya vadesi

---

[252] YILDIRM, a.g.e., s.12.

[253] Gönül KAPAĞAN, "Bağlı Tüketici Kredileri", **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2004, s.24.

süresi 1 yıl olan kredileri ifade eder. Uygulama olarak bir yıla kadar vadelendirilmiş olan krediler kısa vadeli krediler olarak tanımlanır.[254]

2) Orta vadeli krediler: Kredi vade süresi olarak 1 yıl ile 10 yıl arasında olan krediler orta vadeli kredi olarak kabul edilir.

3) Uzun vadeli krediler: Kredi vadesi 10 yıl ve daha fazla sürede olan vadeli kredileri ifade eder. Uzun vadeli kredi sınıfına, vade süresi iki yıl ve daha uzun süreli olan özel, ancak çoğunlukla ticari amaçlı kullandırılan krediler girer. Uzun vadeli kredi türlerinin bazı ülkelerin ilgili regülasyonuna ve/veya ekonomik yapısına bağlı olarak bankacılık sisteminde kabul edilmediği görülmektedir. Uygulama kapsamında uzun vadeli krediler dönem kredileri olarakta nitelendirilebilir.

4.1.3.4 Kullanıldığı Yerlere Göre Kredi Türleri

1) Tarım kredisi: Tarım sektöründe kullanılan ve tarım sektörüne yönelik olarak açılan kredileri ifade eder.

2) Konut kredisi: İnşaat sektörüne faaliyet gösteren ve inşaat projeleri kapsamında kullanılan kredileri ifade eder.

3) Mesleki kredi: Küçük esnaf, sanatkâr ve serbest meslek erbabına açılan kredileri ifade eder.

4) İhracat kredisi: İhraç edilen ürünlerin finansmanını sağlamak amacıyla kullanılan ve/veya kullandırılan için kredileri ifade eder.

4.1.3.5 Kredi Alıcısının Niteliğine Göre Kredi Türleri

1) Kamu kredisi: Kamu tüzel kişilerine (örn. devlet, özel idare, belediye vb.) açılan kredileri ifade eder.

2) Özel krediler: Özel hukuk gerçek ve tüzel kişilerine açılan kredilerdir.

---

[254] KAPAĞAN, a.g.e., s.25.

4.1.3.6 Kredinin Niteliğine Göre Kredi Türleri

1) Nakdi krediler: Para ve para hükmünde değer ifade eden finansal enstrümanların verilmesi kapsamında açılan kredi türlerini ifade eder. Banka tarafından kredi kullandırılan müşteriye nakit ödeme yaparak kredi kullanımının sağlandığı kredi türünü ifade eder. Kredi uygulamaları incelendiğinde, kullandırılan kredilerin büyük bir çoğunluğu nakdi kredilerden oluşmaktadır. Nakdi krediler tür olarak altı alt sınıfa ayrılır. Bunlar:[255]

a) Ödünç: Ödünç kredisi olarak tanımlanan kredilerde, banka tek seferde verdiği krediyi müşteriye öder. Müşteriye verilen kredi miktarı müşteri tarafından iki farklı şekilde ödenebilir. Ödeme şekli tek seferde ve/veya taksitler halinde kredi verene geri ödenebilir. Ödünç kredi türüne örnek olarak müşterilere tahsis edilen meslek kredileri verilebilir. Ödünç kredilerine bir diğer örnek ise kredi kartları gibi dönerli bir şekilde işleyen kredilerdir. Ödünç kredileri olarak kredi kartı uygulaması yoğunlukla kullanılmaktadır. Bu uygulamadaki kredi işlemi, kredi alanın belli bir kredi limitine kadar aldığı kredi miktarını ödemesi durumunda kredi limiti yenilerek yükseltilmekte ve cari hesap şeklinde işlem görmektedir.

b) Senet ve Mal Avansı Kredisi: Bu uygulama içerisinde gerçekleştirilen işlem, verilen kredi miktarının kıymetli evrak aracılığıyla güvence altına alınmasıdır. Bu kredi uygulaması genel olarak kısa süreli olarak yapılır. Kredi kullanan tarafından kullanılan kredi karşılığı kıymetli evrak kredi kullandıran tarafa rehin olarak verilir.

c) Kıymetli Evrakın İştirası veya İskontosu: Belirtilen vade bilgisi kapsamında, vadesi gelmemiş olan ticari senetlerin kalan vadelerine kadar işleyecek faiz ve hizmetin karşılığı olan komisyon tutarı indirilerek, kalan borç bakiyesinin kredi alan tarafa ödenmesine ilişkin oluşan kredi işlemidir.

d) Forfaiting: Kredi kullanacak olan tarafa ait yatırım malı veya hizmet ihracından kaynaklanan alacaklarının uzun vadeli olarak banka tarafından satın alınma işlemini ifade eder. Uygulama olarak vade bilgisi beş veya altı yıllık bir süreyi ifade eder.

---

[255] KAPAĞAN, a.g.e., s.21-23.

Alacak miktarının kredi veren tarafından tahsil edilememesi halinde kredi veren bunu temlik eden (kredi alana) rücu edemeyecektir.

e) Faktoring: Faktoring, faktör tarafından, müşterinin üçüncü şahıs borçlu karşısındaki mal tesliminden veya hizmet edimini ifasından doğan alacaklarını, bedelini alacağın tahsil edileceği zamandan önce peşin olarak ödeyerek, alacağın tahsil edilememesi riskini ve müşteri için borçlunun muhasebesinin tutulması, ihtar işlemleri gibi hizmetlerin üstlenilmesi sureti ile devir ve satın alınmasıdır.

f) Finansal Kiralama: Finansal kiralama, belirli bir süre için kiralayan ile kiracı arasında yapılan ve kiracı tarafından seçilip kiralayan tarafından üreticisinden satın alınan malın mülkiyetinin kiralayanda, kullanımının ise kiracıda belirli bir bedel karşılığında kiracıda bırakıldığı bir işlemdir.

2) Mal şeklindeki krediler: Krediye konu tutarın, sonradan tahsil edilmek üzere ürün olarak verilmesi mal şeklindeki kredileri ifade eder. Müşterilerin yapmış oldukları taksitli satış işlemleri bu kredi türüne örnektir.

3) Maddi olmayan krediler: Kredi alanın itibarını dikkate alarak kredi alanın imzası karşılığında, nakit ya da mal şeklinde olmaksızın kullandırılan kredileri ifade eder.

4.2 Bankalarda Kredi Süreci ve Yönetimi

Kredi yönetiminin geniş bir tanımı şu şekilde yapılabilir:[256]

"Müşteri firmaların finansal davranışları ve pazara yönelme nedenleri sonucu finansal sorunlarının çözümüne yönelik uygun kredinin sunulması, müşteriye finansal danışmanlık işleminin gereği uygulama biçimi ve bununla bağlantılı olarak kredinin fiyatlandırılması, kredi organizasyonu ve analistlerin işbirliği ile derlenen veri ve bilgilerin değerlendirilmesi, kredilendirme sonrası müşteri ilişkilerini ve kredinin takibini kapsayan bir yöntemdir."

[256] YILDIRIM, a.g.e., s.6.

Kredi yönetiminin görev alanları ve yönetim sürecine ait temel aşamalar aşağıdaki gibidir:[257]

- Banka bünyesinde kullanılacak ve/veya kullanılabilir niteliği olan toplam kredi miktarının ve çeşidinin tespit edilmesi,

- Müşterilerin belirlenmesi ve uygun müşterinin seçilmesi,

- Kredi kullandırılması planlanan ve/veya kullandırılmış olan firmalar ile ilgili olarak güvenilir ve çeşitli bilgi kaynaklarından bilgi temin edilmesi,

- Müşterilere ait uygun kredi limitlerinin belirlenmesi,

- Kullandırılan ve/veya kullandırılacak olan kredilere ait güvence çeşitlerinin ve miktarlarının belirlenmesi,

- Müşterilere kredi kullandırımının sağlanması,

- Kredi kullandırım sonrasında kredi ile ilgili olarak gözetim ve kontrol işlemlerinin gerçekleştirilmesi,

- Kredi işlemleri ile ilgili olarak risk yönetim faaliyetinin uygulanması,

Kredi yönetiminin görev alanları değerlendirildiğinde, kredi süreci kapsamında yer alan görevlerin 2 temel görev alanından oluştuğu görülmektedir. Bu işlemler operasyonel ve analitik görev alanlarıdır. Kredi başvurularının incelenmesi, kredi dosyasının oluşturulması, dokümantasyon işlemleri ve raporların oluşturulması gibi işlemler operasyonel bölüm ile ilişkilidir. Kredi işlemlerine ait analitik bölüm; kredi analizi, gözetimi ve kontrolü ile yeni kredi başvurularının analizi, eğitim ve araştırma gibi işlemleri içerir. Analitik bölüme ait faaliyetler spesifik ve uzmanlık gerektiren konulardan oluşmakla birlikte söz konusu işlemlere ait faaliyetlerin konusunda uzman olan personel tarafından yerine getirilmektedir. Analitik faaliyetler, yol gösterici özelliklerinin bulunması açısından diğer operasyonel bölümlerden ayrılmaktadır.

[257] AYANOĞLU ve ERTÜRK, a.g.m., ss.77.

Kredi kullandırma işlemi birden fazla ve çeşit işlemin birlikte gerçekleştirilmesi sonucunda tamamlanmış olur. Kredilendirme süreci, kredi müşterisi ile ilk iletişime geçme ve ilgili müşteri tarafından kredilendirme işlemi için başvuru yapmasıyla başlayan ve kredinin tasfiye edilmesine kadar geçen süreleri ve süreçleri kapsayan işlemlerin bütününü ifade eder.[258]

Bankacılık sektöründe faaliyet gösteren bankaların en temel risklerinden biri olan kredi riski kavramı, kredilendirme sürecinin sonucu ve/veya kredilendirme sürecinin bir parçası olarak karşımıza çıkar. Kredi süreçlerini gerçekleştirilen işlemlere bağlı oluşan riski kavramı, günümüzde teknolojinin gelişmesiyle ve işlemlerin karmaşıklaşması ile birlikte oldukça önemli bir konu haline gelmiştir.

Kredi süreci içerisinde kredi kullanım faaliyetinde bulunulması ve kredi işlemlerine ait temin edilen kaynağın etkin ve verimli bir şekilde kullanılması, ticari ve finansman tüm ekonomik faaliyetlerin bir unsurunu oluşturur. Mevcut durumda banka bünyesinde kullandırılan kredi miktarının bir kısmının donuk bir nitelik alması, bir kısmının da tahsilat işlemlerinde zorluklar yaşanması kredi taleplerinin değerlendirilmesinin önemini ortaya koyar. Bankalar tarafından kredi işlemleri yürütülürken, kredi verme şartlarını ve kriterlerini iyi belirlemelidir. Bu kriterlerin içeriğinde kredi tahsis edilen kredi borçlusunun ve tahsis edilen kredinin yapısı, kullandırım amacı ve geri ödeme durumunun analiz edilebilir nitelikte ve içerikte olması sağlanmalıdır. Banka tarafından kredi miktarını talep eden müşterinin risk profilini ayrıntılı ve titiz bir şekilde değerlendireceği yeterli bilgi kaynağı sağlamalıdır.[259]

Kredinin, bankacılık sektörünün temel işlevlerinden olması nedeniyle; kredi süreçlerinin oluşturduğu riskler, bankacılık sektörünün karşılaştığı en önemli finansal ve operasyonel risk tanımlamalarıdır. Bankaların göstermiş olduğu ve/veya göstereceği performans, krediler süreci içerisinde yer alan yanlış müşteri seçimine ve müşteri seçimine bağlı olarak, müşteri kredi tutarlarının geri dönme olasılıklarının artış ve/veya

---

[258] Hakan ŞAKAR, **Bankalarda Kredilendirme Teknikleri,** 1. Basım, Mida Yayınları, İstanbul, 2002, s.63.

[259] Rıfat T. NALBANTOĞLU, "Türk Bankacılık Sektöründe Krediler ve Muhasebe Denetim Mesleği", **Muhasebe Denetimi Sempozyumu**, İstanbul, 2-6 Mayıs 2001, s.2-3.

azalışlarına bağlıdır. Banka bünyesinde krediler süreci ile ilgili olarak aşağıdaki belirtilen temel aşamalar uygulanır:

a) Kredi Başvuru Talebi: Bankalarda yürütülen kredi işlemleri; kredi başvuru süreci ile başlar. Kredi başvuru süreci içerisinde kredi talebinde bulunan müşteri ile ön görüşme yapılarak, müşteriden kredi başvurusunun değerlendirilmesine ilişkin olarak temel müşteri bilgileri temin edilir. Müşteri, kredi talep aşamasında; bankaya, bankadan temin edeceği krediyi hangi amaçla kullanacağını, krediye ait vade süresini ve tutarını bildirir. Müşteri, bankaya kredi ihtiyacını bizzat iletebileceği gibi, görüşme sırasında da banka, müşterinin kredi ihtiyacını tespit edebilir. Müşteriyle yapılan ön görüşmede, banka kredi politikaları dikkate alınarak müşterinin yapmış olduğu kredi talebi değerlendirilir. Yapılan değerlendirme kapsamında krediye ait geri ödeme şekli ve miktarı belirlenir.[260]

b) Müşteri İstihbaratının ve Kredi Analizinin Yapılması: Müşterinin gerçekleştirmiş olduğu kredi talebi kapsamında ve/veya kredi verilmesi ön görülen müşteriler ile ilgili olarak finansal/finansal olmayan bilgiler temin edilerek, müşteri değerlendirmesi yapılır.

Kredi analizi, kredi talebinde bulunan müşterinin finansal tablolarının incelenmesi faaliyetini kapsar. Bu çalışma kapsamında müşterinin geçmiş, cari ve gelecek dönem içerisindeki faaliyet performansını etkileyen ve etkileyecek bütün faktörlerin değerlendirilmesi yapılır. Bu işlemler gerçekleştirilirken kullandırılacak olan kredinin geri tahsilatının gerçekleştirilebilmesi için gelecek dönem içerisindeki faaliyet sonuçlarının ne şekilde olacağının değerlendirilmesi konusu büyük önem taşır.[261]

c) Kredi Taleplerinin Değerlendirilmesi: Müşteri ile ilgili olarak sağlanan bilgiler çerçevesinde yapılan kredi analizi çalışması, talep edilen kredinin büyüklüğüne ve vade bilgisine göre kredi talepleri değerlendirilir.

---

[260] Ayşegül ÖKER, "Ticari Bankalarda Kredi ve Kredi Riski Yönetimi-Bir Uygulama", **Doktora Tezi**, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2007, s.86.

[261] Ömer Emre TOKEL, "Kredi Risk Modelleri Kullanılarak Kredi Taleplerinin Değerlendirilmesi", **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2004, s.33-42.

d) Teminat Süreci: Krediye ait en önemli kullandırım kriterlerinden biri alınan teminat türü ve miktarıdır. Teminat türü ve niteliğinin önemli olmasının nedeni kullandırılan krediye ait risk derecesini etkilemesinden kaynaklanmaktadır. Müşteriden alınan teminat bedelleri kullandırılan kredi miktarının geri ödenmesi ile ilgili olarak bir güvence oluşturmakla birlikte, teminat bedelini veren taraf adına krediyi ödemesi konusunda motive edici bir unsur oluşturur.[262]

e) Kredinin Maliyetlendirilmesi ve Kredi Kullandırımı: Kredi kullandırımı yapılacak olan müşterinin likidite veya karlılık kriterleri açısından uygun olması durumunda, kredi talepleri değerlendirilmesi aşamasında kredi fiyatlandırılması konusunda müşteriye daha fazla insiyatif kullanılabilmektedir. Kredilendirme aşamasında müşteri tarafından ödenecek olan fiyat, faiz, komisyon ve diğer gider kriterleri kredi maliyeti için önemlidir. Kredi fiyatlandırması aşamasında müşteri ile fiyatlandırma konusunda anlaşılması durumunda, kredi kullandırım süreci uygulanır.

f) Kredi Kullandırımı Sonrasında İzleme ve Kontrol: Kredi izleme ve kontrolü, kredi kullandırım işlemi sonucunda kredi kullandırımı gerçekleştiren tarafın stratejik hedefleri doğrultusunda ulaşmak istediği amaçların ve sorumlulukların-yükümlülüklerin eksiksiz olarak tam, doğru ve zamanında tamamlanıp tamamlanmadığının izlenmesi sürecini içerir. Bu süreç gerçekleştirilirken, işlemlerin verimli bir şekilde yapılması ve izleme sonucunda gerekiyor ise, süreç içerisinde düzeltici önlemlerin alınması sağlanır.[263]

Bankacılık Düzenleme ve Denetleme Kurumu tarafından yayınlanan "Bankaların Kredi Yönetimine İlişkin Rehber" kapsamında kredi riskinin yönetimine ilişkin olarak bankalardan beklenen en iyi uygulamalar açıklamıştır. Belirtilen en iyi uygulamalar tavsiye niteliğinde olmakla birlikte, bankaların organizasyonel yapılarına, stratejik hedef ve beklentilerine göre uygulama olarak farklılık ve çeşitlilik gösterebilmektedir.

Bankaların en kritik operasyonlarından biri olan kredi işlemleri kredi yönetimi faaliyeti ile yürütülür. Banka bünyesinde kredi işlemlerine ait kredi yönetim faaliyeti,

---

[262] ÖKER, a.g.e., s.116.

[263] ÖKER, a.g.e., s.136.

bankanın kredi yönetimine ait stratejileri ve politikaları belirlemesi ile başlamaktadır. Kredi yönetimi faaliyeti içerisinde kredi işlemlerine ait prosedürlerin belirlenmesi ve buna bağlı olarak kredi pazarlama, kredilerin müşterilere tahsis edilmesi işlemleri yer alır. Kullandırılan kredilere bağlı olarak banka tarafından alınan ve/veya alınacak olan kredi risklerinin ölçülmesi, izlenmesi, kontrolünün sağlanması, raporlanması faaliyetleri kredi yönetiminden sorumlu olan üst yönetiminin sorumluluğundadır. Kredi yönetimi kapsamında; alınan riskleri karşılayacak yeterlilikte olan sermayenin banka bünyesinde oluşturulması ve gerekli olan karşılıkların ayrılması faaliyetleri değerlendirilir.[264]

Banka bünyesinde kredi yönetiminden sorumlu olan organizasyonun kredi yönetimine ait görevlerini gerçekleştirirken, banka içerisindeki diğer bölümler ile koordinasyon ve iletişim içerisinde olması gereklidir. Banka içerisinde kredi kullandırımlarına ait üst yönetim tarafından alınan ve/veya alınacak olan kredi kararlarının, sağlam temeller üzerine inşa edilmesi gereklidir. Bu işlemin gerçekleştirilebilmesi için, öncelikli olarak banka içerisindeki bilgi akışı sisteminin iyi oluşturulması gereklidir. Banka bünyesindeki bilgi akış sisteminden etkin ve verimli bir şekilde fayda sağlanmalıdır. Banka bünyesinde sürekli bilgi akışı sağlanması gereken bölümler, muhasebe, bilgi işlem ve hukuk bölümleridir. İlgili bölümlerle bilgi akışının sürekli, düzenli ve tam zamanında bilgi akışını sağlayacak olan yapıların banka bünyesinde oluşturulması gereklidir.[265]

Yayınlanan yönetmelik çerçevesinde; bankalar bünyesinde yürütülen kredi süreçleri ile ilgili olarak uygulanması gereken ilkeler aşağıdaki şekilde belirlenmiştir:[266]

1) Kredi stratejilerinin Oluşturulması: Banka bünyesinde kredi operasyonları ile ilgili olarak stratejiler belirler. Belirlenen stratejilere uygun politika ve uygulama prensipleri geliştirir. Strateji, politika ve uygulama prensipleri yönetim tarafından gözden geçirilmeli ve onaylanmalıdır.

---

[264] BDDK, "Bankaların Kredi Yönetimine İlişkin Rehber", Sayı: 6462, Tarih:17 Eylül 2015, s.1.

[265] AYANOĞLU ve ERTÜRK, a.g.m., ss.77.

[266] BDDK, a.g.e., s.1.

2) Kredi Politikalarının Oluşturulması: Bankalar, organizasyon yapıları içerisinde kullandıkları sistemler ve/veya faaliyetlerin karmaşıklığı ve kredi büyüklüklerine göre kredi politikaları oluşturur. Bu politikalar içerisinde kredinin pazarlanması, müşteriye tahsisi, tahsis edilen kredinin izlenmesi ve takip edilmesi faaliyetleri ve kriterleri yer alır.

3) Kredi Uygulama Yöntemlerinin Prosedür Haline Getirilmesi: Banka bünyesinde; kredi faaliyetlerine ait uygulamalarla ilgili olarak, banka strateji ve politikaları ile uyumlu kredi prosedürleri oluşturulur.

4) Yetki ve Organizasyon Yapısı: Kredi faaliyetlerini banka bünyesinde gerçekleştirecek olan organizasyon yapısı yetki dağılımı sağlanacak bir formatta oluşturulur. Yetki dağılımı, görevler ayrılığı prensibine ve yetki karışıklığına imkân vermeyecek şekilde oluşturulur. Banka bünyesinde oluşturulan organizasyonel yapı içerisinde görev alan bölüm ve çalışanların performansları önceden belirlenmiş kriterler kapsamında izlenir ve ölçümlenir.

5) Dokümantasyon ve Bilgi Sistemleri: Kredi süreçlerine ait banka bünyesinde oluşturulan müşteriye ait bilgiler, müşteri kriteri dikkate alınarak banka bünyesinde görevli ve sorumlu olan kişiler tarafından kolaylıkla erişebilir bir şekilde muhafaza edilir. Kredi yönetim fonksiyonun etkin ve verimli bir şekilde çalışabilmesi için, banka bünyesindeki bilgi sistemlerinin etkin olması sağlanır. Üst yönetim ve kredi faaliyetlerini üstlenen bölümler tarafından kredi işlemlerine ait sorumluluklarını tam, doğru ve zamanında yerine getirebilmesi açısından bilgi sistemlerinden elde edilen verilerin katkısı önemli bir yer tutar. Banka bünyesinde tasarlanan bilgi sistemleri kredi izleme faaliyetlerinin etkinliğini ve verimliliğini artırmakla birlikte; ilgili faaliyetin karmaşıklığı ve büyüklüğü dikkate alınarak oluşturulur.

6) İç Sistemler Kapsamındaki Faaliyetler: Banka bünyesinde yer alan iç sistemler kapsamındaki bölümler kredi yönetim işlemlerine ait operasyonlarını ve faaliyetlerini düzenli olarak inceler ve değerlendirir.

7) Müşterilerin Bilgilendirilmesi: Kredinin pazarlanması ve müşteri tarafından kredi talebinin incelenmesi aşamasında müşteri tarafından kullandırılacak olan

kredi ürünlerinin içeriklerinin tüm yönleri dikkate alınarak, müşterinin doğru bilgilendirilmesi sağlanır.

8) Müşteri Seçimi: Bankanın belirlemiş olduğu kredi politika ve stratejilerine uyumlu bir şekilde müşteri değerlendirmesi ve analizi gerçekleştirilir. Değerlendirme ve analiz sonucu olumlu olan müşteriler ile çalışılır. Kredinin kullandırım amacı, müşterinin ihtiyaçlarına göre banka tarafından ve/veya müşteri tarafından direkt olarak sunulabilir.

9) Değerlendirme: Bankalar tarafından kredi işlemlerinin banka bünyesinde yer alan stratejilere uygun olarak verimli bir şekilde yerinde uygulanabilmesi için önceden belirlenmiş kriterlere göre müşterilerin ölçümlenmesi ve analiz sonuçlarına göre onay mekanizmaları oluşturur. Kredi işlemlerine ait onay işlemleri bankanın üst yönetimi tarafından onaylanmış olan yazılı prosedürlerine uygun olmalıdır. Kredi kullandırılacak olan tarafın banka stratejilerine göre risk değerlendirmesinin yapılabilmesi için, bankanın müşteri ile ilgili olarak yeterli sayıda ve doğru bilgiye sahip olması gereklidir. Kredi tahsis süreci içerisinde ihtiyatlılık kuralı esas olduğundan, bankalar tarafından ekonomik büyüme dönemlerinde bu kuralı olumsuz yönde etkileyecek olan uygulamalardan kaçınılmalıdır.

Bankalar kredilendirme işlemlerinde müşterilerin değerlendirilebilmesi ve buna kaynak oluşturacak olan istihbarat bilgilerinin yapılması için banka bünyesinde mali analiz ve değerlendirme konusunda uzman olan personel bulundurur. Kredilendirme öncesinde kullandırılacak olan kredi miktarının, niteliğinin ve krediyi kullanacak olan müşteriye ait değerlendirme işlemi gerçekleştiren sorumlu kişi tarafından doğru verilere tam ve zamanında ulaşması gereklidir. Müşterinin borç durumu ve kredi tahsisi yapılan kredi miktarının geri ödeme karakteristiği değerlendirilir. Yapılan değerlendirme sonucunda müşterinin kullanabileceği kredi limiti belirlenir. Müşteri limitlerinin dışında müşteri riski değerlendirmesi yapılır. Yapılan analizler kapsamında kredi ihtiyacı ve kredinin kullanım amacı hakkında bilgiler temin edilir. Yapılan değerlendirmeler sonucunda kredi teklifleri yazılı ve detaylı olarak hazırlanır.

Bankanın kullandırmayı hedeflediği krediye ait kredi riski, banka müşterisi ile ilk iletişime geçilmesi aşamasında oluşur. Müşterinin bankaya gelmesi ve/veya diğer alternatif dağıtım kanalları (internet bankacılığı vb.) yoluyla kredilendirme için yaptığı ilk talep aşamasında kredi riski oluşmaya başlar. Bu nedenle, yeni bir kredi kullandırım işlemi ile ilgili olarak girişimde bulunmadan önce kredi müşterisinin iyi tanımlanması ve güven unsurunu taşıdığından emin olunmalıdır. Banka tarafından kredi talebinde bulunan müşterinin kredi koşul ve yükümlülüklerini yerine getirip getiremeyeceğini analiz edebilmek için müşteriye ait kredi kayıtlarını inceler. Müşteri ile ilgili olarak istihbarat işlemleri, referanslar kullanarak ve müşteriye ait finansal kayıtları kontrol edilerek gerçekleştirilir. Bu aşamada değerlendirme ve/veya istihbarat işleminin hatalı yapılması, müşterinin etkin ve verimli bir şekilde analiz edilememesine neden olmakla birlikte; kredi tahsis işlemine ait ana süreç içerisinde, kredilendirme kararının yanlış oluşmasına ve kredi bedelinin yanlış fiyatlandırılmasına neden olabilir. Bu durum kredi ile ilgili olarak daha ilk aşamalarda risklerin ortaya çıkmasına neden olabilir.[267]

Kredi riskinin müşteri değerlendirme aşamasında ortaya çıkmasının engellenmesi amacıyla; banka bünyesinde onaya sunulan kredilerle ilgili olarak hazırlanan müşteri değerlendirme dokümanlarında aşağıdaki belirtilen maddelerin belirtilmesi gereklidir:[268]

- Kredinin kullanım amacı ve geri ödeme için gerekli fon kaynağı,
- Kredi talep eden müşterinin güvenirliliği ve itibarı,
- Müşterinin mevcut risk yapısı, miktarı ve profili, faaliyet gösterdiği piyasa ve ekonomik değişikliklere karşı alabileceği aksiyon kapasitesi,
- Kredinin geri ödenmesi için, müşterinin mevcut finansal durumunun değerlendirilmesi, gelecekteki ve geçmişteki finansal performansının nakit akış yöntemi ile analiz edilmesi,

[267] KOÇYİĞİT ÇİL ve DEMİR, a.g.e., ss.223.

[268] NALBANTOĞLU, a.g.e., s.2-3.

- Müşteri ile ilgili olarak birden fazla ve çeşitte senaryo oluşturularak, müşteriye tahsis edilecek olan kredinin tahsilat kapasitesinin değerlendirilmesi,

- Kredi talebinde bulunan müşterinin geçmiş ve mevcut yasal durumunun incelenmesi ve gerekli olan borç yükümlülüğünü temin edebilme kriterinin değerlendirilmesi,

- Müşteri tarafından ticari kredi talebinde bulunulması durumunda, ticari işletmenin yer aldığı sektör içerisindeki konumu (Pazar payı, üretim hacmi vb.), sektörün genel durumu,

- Kredi talebinde bulunan müşteriye ait oluşturulacak olan kredi sözleşmesinin içerisinde yer alacak olan kredi vade ve koşullarının müşteriye ait mevcut finansal durumu ve gelecekte müşterinin finansal durumunda meydana gelebilecek olan olumsuz ve/veya olumlu değişikliklere istinaden hazırlanması,

- Kredi kullandırımına ait müşteriden temin edilecek olan garanti ve teminatların uygunluğunun ve yeterliliğinin çeşitli senaryolar oluşturularak değerlendirilmesi gereklidir.

10) Müşteri Kredi Limitlerin Belirlenmesi ve Kredi Limitlerine Uyum: Müşterilere ait kredi limitlerinin belirlenmesi işlemi kredi sürecinin en önemli faaliyetini oluşturmaktadır. Kredilerin değerlendirme aşamasında, müşterinin kredi limitlerine olan uygunlukları incelenmeye başlanır. Kredilendirme sürecinin bütün aşamalarında mevzuata ve banka tarafından belirlenmiş düzenleme ve kriterlere uyumu ile ilgili olarak kontrol faaliyeti gerçekleştirilir.

11) Yeniden Yapılandırma: Kredi borcunun ödenmemesine bağlı olarak borç miktarının ödeme süresinin uzatılması aşamasında müşterinin güncel durumdaki kredi kabiliyeti dikkate alınır.

12) Derecelendirme: Kredi riskini yönetmek ve değerlendirmek amacıyla bankalar, banka ölçeği ile uyumlu olarak içsel derecelendirme sistemini oluşturur.

13) Teminat ve Garantilerin Yönetimi: Bankalar karşılaştıkları riskleri minimize edebilmek için, teminat ve garanti araçlarından faydalanabilir. Teminat ve garanti araçlarının kullanılması borçlunun borcunu geriye ödeyebilme kapasitesine bağlıdır. Bu nedenle tazminat ve garanti araçlarının kullanılması, müşterilerin etkin ve verimli bir şekilde değerlendirilmesinde herhangi bir aksaklık yaşanmasına neden olmamalıdır.

14) İzleme Sürecinin Kurulması: Bankalar kredi süreci içerisinde oluşabilecek olan ve/veya oluşan risklerin önlenmesi ve/veya takip edilmesi amacıyla kredi yönetiminin içerisinde kredi izleme yapısı oluşturur.

15) Stres Testleri ve Senaryo Analizleri: Kredi izleme yapısının yanında, karşılaşabilecek olan risklerin analiz edilebilmesi amacıyla stres testleri ve senaryo analizleri oluşturulur. Oluşturulan analiz sonuçları değerlendirilerek alınması gereken önlemler banka bünyesinde oluşturulur.

16) Kredi Takip Süreçlerinin Yönetimi: Bankaların kredi ödeme vadesine uymayan müşterilerine yönelik olarak gerçekleştireceği işlemler ile ilgili olarak politikaları bulunur. Kredi işlemlerine ait uygulanacak olan aksiyon adımları kredi tutarına ait tahsilat etkinliğini sağlayacak nitelikte oluşturulur.

Kredilendirme süreci ile ilgili olarak belirtilen işlemler ve kriterler banka kredi faaliyetlerini yürütürken dikkate alması gereken hususları belirtmekte olup, bu maddeler içerisinde yer alan işlemlerin uygulanması adına gerçekleştirilen kontrol işlemleri, COBIT ve COSO kriterlerinin (COSO küpü) içerisindeki yer alan bileşenlerin bir uzantısı olarak karşımıza çıkmaktadır.

Çalışma kapsamındaki uygulama alanı içerisinde bankalarda kritik ve önemli bir süreç olan kredi faaliyetlerine ait yapılan işlem ve kontroller COBIT ve COSO kontrol modeli bileşenleri dikkate alınarak, risk-kontrol kataloğu ortaya çıkartılmıştır.

5. BÖLÜM
COBIT VE COSO KONTROL MODELİ KAPSAMINDA BANKALARDAKİ KREDİLER SÜRECİNE AİT RİSK KONTROL KATALOĞUNUN OLUŞTURULMASI

5.1 Uygulamanın Amacı ve Kapsamı

Türk bankacılık sektöründe gerçekleştirilen faaliyetlerin birçoğu; bankadan bankaya değişiklik göstermekle birlikte; bankaların bünyesinde bulundurduğu ve/veya dış kaynak kullanımı yoluyla temin ettiği bilgi sistemleri dahilinde faaliyet göstermektedir. Diğer sektörlerde olduğu gibi bankacılık sektöründe de yoğun bilgi kullanımının yanı sıra söz konusu bu bilgilerin değerlendirilmesi analiz edilmesi ve ilgili faaliyete-sürece ait oluşabilecek olan risklerin tespit edilmesi ve tespit edilen risklere yönelik olarak gerekli olan kontrol alanlarının oluşturulması sağlanmalıdır.

Bu nedenle; bankacılık sektöründe bilgi sistemleri ile yürütülen faaliyetlerin bilgi sistemleri denetimi kapsamında, uygulama denetimi ve genel kontrol alanları denetiminin gerçekleştirilerek raporlanması yasal mevzuat açısından talep edilmektedir. Söz konusu bu talep ile ilgili olarak, denetim kapsamında riskli olan alanların değerlendirilmesi ve mevcut durumda ilgili banka tarafından hazırlanmış olan risk ve kontrol kataloglarının incelenerek, gerekli olan denetim çalışmalarının yapılması gerekmektedir.

Yapılan çalışma, söz konusu denetim faaliyetlerine katkı sağlamakla birlikte, denetim faaliyetinin dışında bankacılık sektöründe faaliyet gösteren bankaların bünyesinde yer alan kredi faaliyetlerinin etkin ve verimli bir şekilde yürütebilmesine yardımcı olacaktır.

Tüm bankacılık süreçlerine ait COBIT ve COSO kontrol alanlarının açıklanması çalışmanın kapsamını çok genişleteceğinden, bankacılık sektöründeki bireysel krediler süreci değerlendirilerek, süreç içerisinde oluşabilecek olan riskler tespit edilip, bireysel krediler sürecine ait risk ve kontrol kataloğu oluşturulmuştur. Bireysel krediler sürecine

ait kontrol kataloğu oluşturulurken, COSO ve COBIT kontrol bileşenlerinin birbirleri ile olan ilişkisi dikkate alınmıştır.

Mevcut bankacılık sektöründe yürütülen uygulamalar dikkate alındığında, bilgi sistemlerinin kullanıldığı süreçlerin arttığı ve hatta birçok uygulamanın artık bilgi sistemleri ortamlarında yürütüldüğü ve buna bağlı olarak birçok kontrol uygulamasının otomatik olarak gerçekleştirildiği görülmektedir.

Bağımsız denetimin amacı, bağımsızlık ilkesine bağlı olarak finansal tabloların doğruluğu, tutarlılığı ve tam olarak açıklanmış olması adına makul bir güvence sağlamak ve buna bağlı olarak görüş vermesidir.

Bilgi sistemlerine bağlı olarak yürütülen operasyonların oluşturduğu birçok veri finansal tabloları direkt ve/veya dolaylı olarak etkilemekle birlikte; bankacılık sektöründeki operasyonların bilgi sistemlerine olan bağlılığı değerlendirildiğinde, bankalar tarafından oluşturulan finansal verilerin doğruluğu, tutarlılığı ve tamlığı açısından bilgi sistemleri önemlidir.

Finansal denetim faaliyeti içerisinde süreçlerin iyi bir şekilde analiz edilmesi ve bilgi sistemleri denetim çalışmaları ile finansal denetim çalışmalarının entegre olması gereklidir. Entegrasyon işleminin, bilgi sistemleri denetim ve test işlemleri sonucunda elde edilen sonuçların, finansal denetim kapsamında değerlendirilmesi gereklidir. Bilgi sistemleri kapsamında finansal veri üretimiyle ilgili olan süreç ve sistemler içerisindeki kontrollerin mutlak suretle değerlendirilmesi gereklidir.

Bu kapsamda uygulamanın ana problemi, bankacılık sektöründe faaliyet gösteren bankaların süreçlere ait risk ve kontrol katalogları oluşturulmuş olmasına rağmen COSO ve COBIT bileşenleri açısından değerlendirilerek, ilgili bileşenler ile bağlantıları kurulmamakla birlikte, söz konusu bu bağlantılara bağlı olarak süreç kapsamında etkin bir şekilde test edilmesi gereken faktörlerin bir haritası oluşturulmamaktadır.

Çalışma kapsamında bu bağlantının kurulması sağlanmakla birlikte, ideal bir bireysel kredi süreci içerisindeki risk faktörlerinin hangi kontrol işlemleri ile bağlantılı olarak ne şekilde test ve kontrol edileceği açıklanmıştır.

5.2 Krediler Sürecine Ait Temel Risk Tanımlamalarının COSO - COBIT Kontrol Hedefleri ile Bağlantısı

COBIT ve COSO standartlarının birbirleriyle olan ilişkileri değerlendirildiğinde, ilgili standartlara ait kontrollerin ve buna bağlı olarak gerçekleştirilmesi gereken işlemlerin temel hedefi; işletme bünyesinde yürütülen işlemlerin öncelikli olarak etkin ve verimli bir şekilde yürütülmesi, yasal otoriteler tarafından belirlenen kanun ve düzenlemelere tam, doğru ve zamanında uyum sağlamanın yanı sıra, şirket bünyesinde gerçekleştirilen operasyonel faaliyetlere bağlı olarak operasyonel faaliyet sonuçlarının yer aldığı güvenilir finansal tabloların oluşmasını sağlamaktır.

Bu nedenle, COBIT ve COSO standartları bankacılık sektöründe oluşan operasyonel riskler başta olmak üzere finansal ve yasal risklerin minimize edilmesinde ve/veya önlenmesinde rol oynamaktadır. Bankacılık sektöründe uygulanan faaliyetlerin etkin ve verimli bir şekilde yürütülmesi amacıyla tasarlanan ve uygulanan kontroller, ilgili standartların belirttiği şekilde kontrollere uygulanmıştır.

Bankacılık sektöründe faaliyet gösteren bir bankanın krediler süreci ile ilgili temel olarak karşılaşabileceği risk tanımlamaları aşağıda belirtilmiş olup, COBIT ve COSO standartlarının ilgili banka bünyesinde uygulanması durumunda söz konusu risk faktörleri minimize edilebilir ve/veya önlenebilmektedir.

Süreç: Kredi Risk Yönetimi

Alt Süreç: Kredi Yönetimi

İş Hedefi: Müşterilere verilen kredilere istinaden alınan teminatların sürekli olarak izlenmesi ve takip edilmesi

Risk: Müşteriden alınan teminatların değer kaybetmesine bağlı olarak müşteriden alınan teminat değerlerinin finansal tablolara yeni değeri ile birlikte tam, doğru ve zamanında yansıtılmaması

Risk Türü: Finansal, Operasyonel ve Yasal

Kontrol (ler):

1) Önceden oluşturulmuş olan güvenlik seviyesinde bağlı olarak, müşteriden alınan teminat değeri ile müşteri kredi limit değeri arasındaki fark değerinin, güvenlik seviyesini aşması durumunda, bankacılık sistemi tarafından istisna raporu oluşturulur. Bu rapor, banka bünyesinde yer alan sorumlu ve yetkin bir personel tarafından gözden geçirilerek kontrol edilir.

Kontrol Türü: Belirleyici (Tespit Edici)-Otomatik-Manuel Kontrol

COSO maddesi: Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma c) AI6-Değişiklik Yönetimi d) DS5-Sistem Güvenliğinin Sağlanması e) DS9-Konfigürasyon Yönetimi, f) DS11-Veri Yönetimi, g) ME2-İç Kontrolün İzlenmesi ve Değerlendirilmesi

2) İlgili işkolu tarafından özellikle iptal edilmemiş olan kredi müşterileri için banka bünyesinde yer alan bütün yüksek riskli ve tutarlı olan krediler için yıllık

kredi izlemeleri yapılır. Kredi komitesi tarafından yüksek riskli ve yüksek tutarda olan müşteri hesaplarına ait teminat değerleri düzenli-periyodik olarak takip edilir.

Kontrol Türü: Önleyici-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Risk Değerlendirme, İzleme

COBIT maddesi: -

3) Yönetimin, müşteri kredi notunun belirlenmesinde dikkate alınan teminatı bağımsız değerlendirme ve yorumlama fonksiyonu bulunur.

Kontrol Türü: Önleyici-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri

COBIT maddesi: -

4) Banka bünyesinde yer alan kredilerdeki bozulmalar (temerrüte düşen kredi bilgileri, tahsilat problemleri vb.) yönetim tarafından periyodik olarak gözden geçirilir ve onaylanır.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel-Otomatik Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri

COBIT maddesi:

a) AI2-Uygulama yazılımının geliştirilmesi ve bakımı, b) DS5-Sistem Güvenliğinin Sağlanması, c) DS9-Konfigürasyon Yönetimi, d) DS11-Veri Yönetimi

5) Banka bünyesinde yer alan kredi komitesi, bankanın stratejik ve sahip olduğu risk profilinin krediler bölümü tarafından gözden geçirilmesini ve raporlanmasını sağlar.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, İzleme

COBIT maddesi: -

Süreç: Kredi Risk Yönetimi

Alt Süreç: Kredi Yönetimi

İş Hedefi: Müşterilere verilen kredilere istinaden alınan teminatların sürekli-periyodik olarak izlenmesi ve takip edilmesi

Risk: Bireysel kredi kullananlarının kredibilitesinin düşüş göstermesi

Risk Türü: Finansal

Kontrol (ler):

1) Önceden belirlenmiş ve sistem içerisine tanımlanmış olan ayarları geçersiz kılmak için sistem konfigürasyonlarının oluşturulması ve/veya risk değerlendirme limitlerinin uygun ve yetkili personeller ile sınırlandırılması

Kontrol Türü: Önleyici-Otomatik Kontrol

COSO maddesi: Kontrol Faaliyetleri, Bilgi ve İletişim

COBIT maddesi:

a) DS1-Hizmet Seviyelerini Tanımlama ve Yönetme, b) DS7- Kullanıcıların Eğitilmesi, c) DS9-Konfigürasyon Yönetimi, d) DS5-Sistem Güvenliğinin Sağlanması, e) DS11-Veri Yönetimi

2) Banka bünyesinde oluşturulmuş olan bir kredi derecelendirme sistemi, müşterilerin kredi faaliyetlerindeki riskleri ve kredi kalitelerinin değerlendirilmesinde bir çerçeve sunar.

Kontrol Türü: Önleyici-Otomatik Kontrol

COSO maddesi: Kontrol Faaliyetleri

COBIT maddesi:

a) AI2- Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) DS4-Hizmet Sürekliliğinin Sağlanması, c) DS5-Sistem Güvenliğinin Sağlanması d) DS9-Konfigürasyon Yönetimi, e) DS11-Veri Yönetimi

3) Taahhütlerini yerine getirmeyen kredi müşterileri için sistem tarafından oluşturulan istisna raporu, bağımsız kredi bölümü personeli tarafından gözden geçirilir ve sorumlu bir personel tarafından periyodik olarak takip edilir.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel-Otomatik Kontrol

COSO maddesi: Kontrol Ortamı, Risk Değerlendirme, Kontrol Faaliyetleri

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma c) AI6-Değişiklik Yönetimi d) DS5-Sistem Güvenliğinin Sağlanması e) DS9-Konfigürasyon Yönetimi, f) DS11-Veri Yönetimi, g) ME2-İç Kontrolün İzlenmesi ve Değerlendirilmesi

4) Sistem içerisinde yer alan müşteri ana veri dosyasında yapılan değişiklikler yetkilendirilir ve sistem içerisinden izlenebilir.

Kontrol Türü: Önleyici-Otomatik Kontrol

COSO maddesi: Kontrol Faaliyeti, İzleme

COBIT maddesi:

a) AI6-Değişiklik Yönetimi, b) DS1-Hizmet Seviyelerini Tanımlama ve Yönetme, c) DS5-Sistem Güvenliğinin Sağlanması, d) DS9-Konfigürasyon Yönetimi, e) DS11-Veri Yönetimi, f) ME2-İç Kontrolün İzlenmesi ve Değerlendirilmesi

5) Hata raporları yönetim tarafından periyodik olarak gözden geçirilmekte ve kredi bölümündeki bağımsız bir kredi personeline raporlanır.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel Kontrol

COSO maddesi: Kontrol Faaliyetleri, Bilgi ve İletişim, İzleme

COBIT maddesi: -

6) Krediler sürecinde yer alan ilişkili her bir bölüm, yönetim süreçlerinin belirlenmesi, gözden geçirilmesi ve operasyonlardaki kalitenin etkinliğini kaybetmesine bağlı olarak risk kayıplarının raporlanabilmesi amacıyla bir izleme listesinin kurulmasından sorumludur.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, İzleme

COBIT maddesi: -

7) Müşteriler tarafından ödenmemiş olan kredilerin oluşması durumu banka bünyesinde özel bir durum olarak nitelendirilmekle birlikte, ödenmemiş olan kredi bilgileri banka bünyesinde yer alan sorumlu bir personel tarafından periyodik olarak incelenir ve takip edilir.

Kontrol Türü: Belirleyici-Manuel-Otomatik Kontrol

COSO maddesi: Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:

a) DS5-Sistem Güvenliğinin Sağlanması, b) DS11-Veri Yönetimi

8) Yönetim, banka bünyesinde müşterilere ait kredi derecelendirme notunun uygun değerlendirilip, gözden geçirildiği bağımsız bir kredi izleme fonksiyonuna sahip olmalıdır.

Kontrol Türü: Önleyici-Manuel-Otomatik Kontrol

COSO maddesi: Risk Değerlendirme

COBIT maddesi:

a) DS5-Sistem Güvenliğinin Sağlanması, b) DS11-Veri Yönetimi

Süreç: Kredi Risk Yönetimi

Alt Süreç: Kredi İzleme

İş Hedefi: Müşterilere verilen kredilerle ilgili olarak, kredi tutarına ait ilk sağlanan kaynak bedeli ile birlikte müşteri ile kredi ilişkisinin sürekli olarak takip edilmeye başlanması

Risk: Müşteriye sağlanan kredi notu ve/veya limit bilgisinin uygunluğunun takip edilmemesi,

Risk Türü: Finansal ve Operasyonel

Kontrol (ler):

1) Yönetim ve/veya Kredi İzleme Bölümü, Krediler Bölümü personeli tarafından kredi derecelendirilmesi yapılan ve/veya müşterilere ait kredi derecelendirilmesi değiştirilen müşterilere ait sistem değişikliklerinin tam, doğru ve zamanında yapıldığından emin olur.

Kontrol Türü: Belirleyici (Tespit Edici)-Otomatik Kontrol

COSO maddesi: Kontrol Ortamı, Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:

a) DS5-Sistem Güvenliğinin Sağlanması, b) DS11-Veri Yönetimi, c) ME2- İç Kontrolün İzlenmesi ve Değerlendirilmesi

2) Kredi risk yönetimi, kredi bölümü tarafından hazırlanan kredi izleme listesini gözden geçirir.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel Kontrol

COSO maddesi: Kontrol Faaliyetleri, İzleme

COBIT maddesi: -

3) Kredi borçlularına ait kredi notu bilgilerine ait güncel bilgi eksikliklerine ait hazırlanan/düzenlenen istisna raporları, uzman bir personel tarafından gözden geçirilir ve takip edilir.

Kontrol Türü: Önleyici-Manuel Kontrol

COSO maddesi: Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:

a) DS5-Sistem Güvenliğinin Sağlanması, b) DS11-Veri Yönetimi

4) Yönetim, müşterilere sağlanan kredileri gözden geçiren ve verilen kredilerin müşterilere ait belirlenen kredi notları ile uygun bir şekilde sağlandığını onaylayan, bağımsız bir kredi izleme fonksiyonuna sahiptir.

Kontrol Türü: Önleyici-Manuel-Otomatik Kontrol

COSO maddesi: Risk Değerlendirme

COBIT maddesi:

a) DS5-Sistem Güvenliğinin Sağlanması, b) DS11-Veri Yönetimi

5) Müşterilerin kredi notları ile ilgili olarak yapılan otomatik değişikliklere ait sistem konfigürasyonları (yapılandırmaları) düzgün tasarlanmış, uygulanmış, işlevsel, korunaklı ve kontrol prosedürlerindeki değişikliklere uygundur.

Kontrol Türü: Önleyici- Otomatik Kontrol

COSO maddesi: Kontrol Faaliyetleri

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma, c) AI6-Değişiklik Yönetimi d) AI7- Sistem Çözümlerinin, Değişikliklerinin Uygulanması ve Akredite Edilmesi e) DS5-Sistem Güvenliğinin Sağlanması, f) DS9-Konfigürasyon Yönetimi, g) DS11- Veri Yönetimi,

6) Sistem konfigürasyonları (yapılandırması) uyarı-hata iletileri ile ilişkili olup, düzgün tasarlanmış, uygulanmış, işlevsel, korunaklı ve kontrol prosedürlerindeki değişikliklere uygundur.

Kontrol Türü: Önleyici- Otomatik Kontrol

COSO maddesi: Kontrol Faaliyetleri, Bilgi ve İletişim

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma, c) AI6-Değişiklik Yönetimi d) AI7- Sistem Çözümlerinin, Değişikliklerinin Uygulanması ve Akredite Edilmesi e) DS5-Sistem Güvenliğinin Sağlanması, f) DS9-Konfigürasyon Yönetimi, g) DS11- Veri Yönetimi,

Risk: Müşteriye ait kredi derecelendirme bilgilerinin bankacılık sistemi içerisinde tam, güncel ve doğru bir şeklide yer almaması

Risk Türü: Finansal ve operasyonel

Kontrol (ler):

1) Sistem içerisinde yer alan müşteri kredi derecelerine/notlarına olan erişim ve yetkilendirme işlemleri görevler ayrılığı ilkesine göre ayrıştırılmıştır.

Kontrol Türü: Önleyici- Otomatik Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri

COBIT maddesi:

a) AI4-Operasyona Olanak Sağlama ve Kullanma, b) DS5-Sistem Güvenliğinin Sağlanması, c) DS9-Konfigürasyon Yönetimi,

2) Müşteriler tarafından ödenmemiş olan kredilerin ortaya çıkması durumu özel bir durum olarak tanımlanmakla birlikte, ödenmemiş olan kredi bilgileri banka bünyesinde yer alan yetkin bir personel tarafından periyodik olarak incelenir ve takip edilir.

Kontrol Türü: Belirleyici-Manuel-Otomatik Kontrol

COSO maddesi: Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:

a) DS5-Sistem Güvenliğinin Sağlanması, b) DS11-Veri Yönetimi

3) Müşterilerle ilgili etkin ve verimli bir takip gerçekleştirebilmek için, bankacılık sistemi tarafından oluşturulan müşteri kredi derecelendirme bilgilerindeki değişiklikler ve kredi izleme listesinde yer alan müşteriler Krediler Bölümü tarafından analiz edilir.

Kontrol Türü: Önleyici- Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Bilgi ve İletişim, İzleme

COBIT maddesi: -

4) Banka yönetimi, müşterilere verilen ilk kredi derecelendirme notunun uygun olduğu sonucuna varabilmek amacıyla bağımsız bir kredi izleme fonksiyonuna sahiptir.

Kontrol Türü: Belirleyici- Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri

COBIT maddesi: -

5) Bankacılık sistemi içerisindeki müşteri kredi derecelendirmelerindeki değişikliklere ait sistem erişimleri, düzgün tasarlanmış, uygulanmış, işlevsel, korunaklı ve kontrol prosedürlerindeki değişikliklere uygundur.

Kontrol Türü: Önleyici- Otomatik Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri,

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma, c) AI6-Değişiklik Yönetimi d) AI7- Sistem Çözümlerinin, Değişikliklerinin Uygulanması ve Akredite Edilmesi e) DS5-Sistem Güvenliğinin Sağlanması, f) DS9-Konfigürasyon Yönetimi, g) DS11- Veri Yönetimi,

6) Bankacılık sistemi içerisindeki müşteri kredilerinin sınıflandırılmasında kullanılan standart ve otomatik kredi kategorizasyonu ile ilişkili olan sistem konfigürasyonu (yapısı), düzgün tasarlanmış, uygulanmış, işlevsel, korunaklı ve kontrol prosedürlerindeki değişikliklere uygundur.

Kontrol Türü: Önleyici- Otomatik Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma, c) AI6-Değişiklik Yönetimi d) AI7- Sistem Çözümlerinin, Değişikliklerinin Uygulanması ve Akredite Edilmesi e) DS5-Sistem Güvenliğinin Sağlanması, f) DS9-Konfigürasyon Yönetimi, g) DS11- Veri Yönetimi,

Süreç: Kredi Risk Yönetimi

Alt Süreç: Kredi Portföy Yönetimi

İş Hedefi: Kredi kayıplarının ve tahsis edilen kredi risklerinin minimize edilmesi

Risk: Kredi pozisyonlarının ve dağılımlarının (yoğunlaşmalarının) kontrol edilmemesi

Risk Türü: Finansal, Yasal

Kontrol (ler):

1) Kredi portföyündeki yoğunlaşma oranlarının düzenli olarak takip edilmekle birlikte, istinai görülen kredi ürünleri; söz konusu ürünlere özgü olan periyodik olarak belirlenen zaman periyotlarında takip edilir.

Kontrol Türü: Önleyici-Otomatik-Manuel Kontrol

COSO maddesi: Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma, c) AI6-Değişiklik Yönetimi d) AI7- Sistem Çözümlerinin, Değişikliklerinin Uygulanması ve Akredite Edilmesi e) DS5-Sistem Güvenliğinin Sağlanması, f) DS9-Konfigürasyon Yönetimi, g) DS11- Veri Yönetimi,

2) Sektörel risk ve pozisyonlar (ortaya çıkması beklenen risk kayıpları) Kredi Risk Komitesi tarafından aylık olarak incelenir.

Kontrol Türü: Önleyici-Otomatik-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:

a) AI4-Operasyona Olanak Sağlama ve Kullanma, b) DS5-Sistem Güvenliğinin Sağlanması, c) DS9-Konfigürasyon Yönetimi, d) DS11- Veri Yönetimi, e) ME2-İç Kontrolün İzlenmesi ve Değerlendirilmesi

3) Banka bünyesinde uygun taşınan pozisyonlara sahip olunması için kredilere ait yoğunlaşma riski, risk yönetimi tarafından incelenir.

Kontrol Türü: Önleyici-Otomatik-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Risk Değerlendirme, İzleme

COBIT maddesi:

a) DS11- Veri Yönetimi

4) Taşınan kredi pozisyonlarına ait taşınan risk limitleri ile ilişkili olan sistem konfigürasyonları (yapılandırması) düzgün tasarlanmış, uygulanmış, işlevsel, korunaklı ve kontrol prosedürlerindeki değişikliklere uygundur.

Kontrol Türü: Önleyici-Otomatik Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma, c) AI6-Değişiklik Yönetimi d) AI7- Sistem Çözümlerinin, Değişikliklerinin Uygulanması ve Akredite Edilmesi e) DS5-Sistem Güvenliğinin Sağlanması, f) DS9-Konfigürasyon Yönetimi, g) DS11- Veri Yönetimi,

5) Krediler Bölümü'nde yer alan ilgili iş kolları tarafından, kredi kayıp oranları ve tahsilatı mümkün olmayan kredi bilgileri düzenli olarak incelenir ve takip edilir. Müşterilere sağlanan kredi bilgilerinden sıra dışı işlem/faaliyet gösteren kredi bilgileri periyodik olarak (zaman bazlı) incelenir ve takip edilir.

Kontrol Türü: Önleyici-Otomatik-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, İzleme

COBIT maddesi:

a) DS11- Veri Yönetimi, b) ME2-İç Kontrolün İzlenmesi ve Değerlendirilmesi

Süreç: Kredi Risk Yönetimi

Alt Süreç: Müşteri kredi zararları ile ilgili olarak karşılık ayrılması

İş Hedefi: Bankaya ait kredi zararlarına ait rezerv pozisyonlarının finansal tablolarda doğru bir şekilde raporlanması

Risk: Bankaya ait artık risk pozisyonun finansal tablolara tam, doğru ve zamanında yansıtılmaması (finansal tablolarda yer alan kredi zararına ait rezerv miktarının portföydeki kayıpları yansıtmaması)

Risk Türü: Finansal ve Yasal

Kontrol (ler):

1) Kredi zararı oluşan kredi bilgilerinden kredi zarar tutarı ileriye taşınabilen krediler, kredi bölümü bünyesindeki iş birimi tarafından üç ayda bir düzenlenerek kredi zararı tutarı ileri taşınır.

Kontrol Türü: Önleyici-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri, İzleme

COBIT maddesi: -

2) Banka bünyesinde kredi zararlarına ait düzeltme işlemlerinin gerçekleştirildiği sistem içerisinde erişim ve bilgi girişi yetkilendirmeleri uygun bir şekilde ayrıştırılmıştır.

Kontrol Türü: Önleyici-Otomatik Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri

COBIT maddesi:

a) DS5-Sistem Güvenliğinin Sağlanması, b) DS11- Veri Yönetimi,

3) Kredi Risk Yönetimi tarafından ödenmemiş olan kredi miktarının kredi zarar rezervine oranı, itfa edilen (zarar olarak kayıt edilen) kredi miktarının kredi rezerv karşılığına oranı gibi anahtar performans ölçümleri gözden geçirilir.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi: -

4) Banka bünyesinde önceden belirlenmiş ve oluşturulmuş olan matris/kontrol kataloğu dahilinde; kredi portföyü içerisinde belirli gereksinimleri karşılayan krediler, otomatik olarak karşılık ayrılmayacak olan krediler statüsünde yer alır.

Kontrol Türü: Önleyici-Otomatik Kontrol

COSO maddesi: Kontrol Faaliyetleri, İzleme

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma, c) AI6-Değişiklik Yönetimi d) AI7- Sistem Çözümlerinin, Değişikliklerinin Uygulanması ve Akredite Edilmesi e) DS5-Sistem Güvenliğinin Sağlanması, f) DS9-Konfigürasyon Yönetimi, g) DS11- Veri Yönetimi,

5) Tarihsel kredi kayıplarına ait kredi verileri kullanılarak hesaplanan beklenen kredi kayıp seviyesi ile ilişkili oluşturulan model konfigürasyonları

(yapılandırması) düzgün tasarlanmış, uygulanmış, işlevsel, korunaklı ve kontrol prosedürlerindeki değişikliklere uygundur.

Kontrol Türü: Önleyici-Otomatik Kontrol

COSO maddesi: Kontrol Faaliyetleri

COBIT maddesi:

a) AI2-Uygulama Yazılımının Geliştirilmesi ve Bakımı, b) AI4-Operasyona Olanak Sağlama ve Kullanma, c) AI6-Değişiklik Yönetimi d) AI7- Sistem Çözümlerinin, Değişikliklerinin Uygulanması ve Akredite Edilmesi e) DS5-Sistem Güvenliğinin Sağlanması, f) DS9-Konfigürasyon Yönetimi, g) DS11- Veri Yönetimi,

6) Karşılık etkenleri, rezerv metodolojilerinin onaylanması süresi boyunca yönetim tarafından gözden geçirilir ve karar verilir.

Kontrol Türü: Önleyici-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:-

7) Kredi rezervlerine ait bir sürecin parçası olan ve değer düşüklüğüne uğrayan herhangi bir kredinin bulunup bulunmadığını belirlemek için müşteri ilişkileri yöneticileri tarafından kayıp değerlendirme raporu 3'er aylık dönemlerin sonunda tamamlanır.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi:-

8) Risk Danışmanlık İzleme Komitesi tarafından grup izleme değerlendirmesi yaparken, her bir iş birimi için oluşturulan kayıp tahmin modellerinin ve değerlendirmelerin uygunluğunu gözden geçirir.

Kontrol Türü: Önleyici-Manuel Kontrol

COSO maddesi: Risk Değerlendirme, Kontrol Faaliyetleri, İzleme

COBIT maddesi: -

9) Banka yönetimi tarafından, finansal tablolarla ve finansal tablo açıklamaları ile ilişkili olan önemli muhasebe hareketleri, muhasebe ve raporlama standartlarına uygunluk açısından incelenir ve kontrol edilir.

Kontrol Türü: Belirleyici (Tespit Edici)-Manuel Kontrol

COSO maddesi: Kontrol Ortamı, Kontrol Faaliyetleri

COBIT maddesi: -

5.2.1 Krediler Süreci İle İlişkili Olan İş Akış Şemaları

Banka bünyesinde yürütülen işlemlerle ilgili olarak iş akış şemalarının oluşturulması ve üst yönetim tarafından onaylanmış olan iş akış şemalarının banka bünyesinde duyurulması sağlanmalıdır. İş akış şemalarından yer alan bilgilerin banka bünyesinde uygulanıp uygulanmadığı periyodik olarak sorgulanmalıdır. Bu işlem banka bünyesinde oluşturulan iç kontrol yapısından talep edilen kriterlerin sağlanması için önem arz eder. Banka bünyesinde oluşturulan iş akış şemalarında iş süreçleri bazında kontrollerin, iş adımlarının belirtilmesi ve banka bünyesinde belirlenen strateji ve hedef kapsamında güncellenmesi sağlanmalıdır.

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
1	İş Akışları					Bireysel Krediler Süreci İş Akışları								
1.1	İş Akışları	OK	Belirleyici	Bireysel Krediler	XXX	Bireysel Krediler Süreci'ne ilişkin güncel iş akışları bulunmaktadır. Bireysel krediler sürecine ait iş akışları XXX sisteminde güncellenmekte ve süreçle ilgili olan bütün birimlere güncelleme bilgileri iletilmektedir. Bireysel krediler sürecine ait güncelleme faaliyetine ait bilgiler XXX sistemi içerisinde takip edilir. XXX sisteminde güncellemenin hangi bölüm tarafından ne zaman ve hangi tarihte gerçekleştirildiği bilgisi yer almaktadır.	Bankaların İç Sistemleri Hakkında Yönetmelik	İhtiyaç Bazlı	Yıllık	Bireysel Krediler Süreci'ne ilişkin kontrol noktalarının ve iş adımlarının gösterildiği iş akış şemalarının varlığı ve güncelliği kontrol edilir.	Tüm Popülasyon	Banka bünyesinde gerçekleştirilen bireysel kredi operasyonları ile ilgili olarak operasyon iş adımlarını anlatan ve üst yönetim tarafından onaylanmış olan iş akış şemalarının bulunmaması ve/veya güncel versiyonlarının ilgili kişilere bildirilmemesi banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Bilgi ve İletişim

5.2.2 Kredi Başvuru, Değerlendirme ve Tahsis Süreci

Bankaların temel faaliyetlerinden biri kredilendirme sürecidir. Bankaya ait faaliyetlerden kaynaklanan gelirlerin büyük dilimini kredilendirme faaliyetlerine bağlı olarak oluşan faiz ve komisyon kalemleri oluşturmaktadır. Bu bilgiden hareket ile kullandırımı yapılan kredilere ait anapara ve faiz giderlerinin ödenmemesi, bankalar açısından önem derecesi yüksek olan bir risk haline gelmektedir. Kredi kullandırım işlem ve kararları ile ayrıntılı ve hassas çalışma yapılması, kredi riskinin tamamen ortadan kaldırılmasına olanak sağlamaz. Bu nedenle bu riski azaltmak amacıyla bankalar kredi vermeden önce kredi talep edenin uygunluğunu değerlendirmesi gereklidir. Bunun için öncelikle kredi talep edenin banka tarafından net bir şekilde tanınması önemli bir aşamadır. Bu aşamanın en önemlisi istihbarat ve finansal analiz çalışmalarıdır. Kredi taleplerinin analiz faaliyeti, bankanın vereceği kredilerin tahsilatına istinaden gerçekleştirilen inceleme ve değerlendirmelerdir. Bu değerlendirmelerin tam, doğru ve zamanında yapılabilmesi amacıyla müşteriden temin edilen bilgilerin doğru ve net olması önemlidir. Bu nedenle, bankalar tarafından kredi faaliyetlerinin verimli bir şekilde oluşturulması amacıyla banka bünyesinde analiz, değerlendirme ve onay mekanizmaları oluşturulur. Banka bünyesinde oluşturulan değerlendirme ve onay işlemleri bankanın kredi politikası ile uyumlu olup, söz konusu sürece ait işlemler banka tarafından belirlemiş olup, stratejilere göre değişkenlik gösterebilir.

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
2	Kredi Başvuru, Değerlendirme Tahsis					Bireysel kredi başvurularının (taşıt, ihtiyaç, konut kredileri) değerlendirilmesi ve tahsis süreci kapsamındaki kontroller								
2.1	Kredi Başvuru, Değerlendirme Tahsis	OK	Belirleyici	Bireysel Krediler	XXX	Banka'nın bireysel krediler süreci kapsamında güncel kredi başvuru ve tahsis prosedürleri ve uygulama talimatları mevcuttur. Söz konusu uygulama talimatları ve tahsis prosedürleri XXX sistemi içerisinde yer almaktadır. XXX sistemi içerisinde yer alan uygulama talimatları ve tahsis prosedürleri periyodik olarak güncellenmekte ve periyodik olarak güncelleme işlemleri XXX sistemi üzerinden kredi başvuru, değerlendirme ve tahsis işlemleri ile sorumlu olan bölümlerle paylaşılmaktadır. XXX sisteminde gerçekleştirilen güncellemelerinin hangi bölüm tarafından ne zaman ve hangi tarihte gerçekleştirildiği bilgisi yer almaktadır.	-	İhtiyaç Bazlı	Yıllık	Banka'da bireysel kredi başvuru ve tahsis işlemlerine ilişkin kılavuz dokümanların (manüel, prosedür, politika vs.) varlığı ve güncelliği periyodik olarak kontrol edilir.	Tüm Popülasyon	Bireysel kredi operasyonları ile ilgili olarak güncel kılavuz dokümanlarının banka bünyesinde yer almaması, operasyonel işlemlerin etkin ve verimli bir şekilde gerçekleştirilememesine dolayısıyla banka bünyesinde finansal ve operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Bilgi ve İletişim
2.2	Kredi Başvuru, Değerlendirme Tahsis	MK-OK	Belirleyici	Bireysel Krediler	YYY	Bireysel kredi başvuruları müşteri tarafından eksiksiz doldurulmuş ve imzalanmış "Bireysel Krediler Başvuru Formu" ile yapılmaktadır. Ayrıca, başvurunun geçerli olabilmesi ve değerlendirilmesi için kredi talebinde bulunan müşteri ve kefil (varsa) tarafından Bireysel Krediler Uygulama Esasları "Kredi Başvurusu Sırasında İstenen Belgeler" bölümünde belirtilen dokümanlar temin edilmektedir. Temin edilen dokümanlara ait bilgiler YYY sistemi içerisinde tanımlanmaktadır.	-	İşlem Bazlı	Yıllık	Banka'da bireysel kredi başvuru süreci ve bireysel kredi başvurusu yapılan kaynak noktalar sorgulanır. Sistem üzerinden denetim dönemi kapsamında tahsis edilen kredi listesi alınır. Denetim dönemi içerisinde müşterilere ait seçilen 25 adet örneklem için müşteri tarafından eksiksiz doldurulmuş ve imzalanmış "Bireysel Krediler Başvuru Formu"	25	Müşteriler tarafından bankaya yapılan bireysel kredi başvuru işlemleri ile ilgili olarak doldurulması gereken bilgi ve belgelerin eksik, hatalı ve/veya yanlış bir şekilde doldurulması, müşterilerle ilgili bilgilerin banka bünyesinde tam ve doğru bir şekilde yer almamasına bu nedenle; banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										aranır. Ayrıca, seçilen örneklem kapsamında başvuru sırasında istenen belgelerin alınmış olduğu teyit edilerek, müşterilere ait bilgilerin ilgili bankacılık sistemine tam, doğru ve zamanında girildiği kontrol edilir.				
2.3	Kredi Başvuru, Değerlendirme Tahsis	MK	Belirleyici	Bireysel Krediler	-	Bireysel Portföy Yöneticisi (Yetkilisi/Yetkili Yardımcısı) müşterinin teslim ettiği belgelerle "Bireysel Krediler Başvuru Formu"nda beyan edilen bilgilerin uyumunu ve doğruluğunu kontrol ederek, başvuru formu üzerinden müşterinin aylık ödeyebileceği taksitleri, toplam gelir ve giderlerini, ibraz edilen belgelerle karşılaştırarak ön değerlendirme yapmaktadır. Ön değerlendirme sonuçları ile ilgili olarak Bireysel Bankacılık Müdürü / Bireysel Portföy Yöneticisi (Yönetmeni/Yetkilisi) ve Şube Müdürü bilgilendirilmektedir.	-	İşlem Bazlı	Yıllık	Şubede yapılan bireysel kredi başvuruları ile ilgili "ön değerlendirme süreci" süreç sahipleri ile görüşülerek incelenir. Denetim dönemi kapsamında "sistem" üzerinden yapılmış olan "bireysel kredi başvuru listesi" temin edilir. Denetim dönemi itibariyle seçilen 25 adet başvuru için ön değerlendirme yapılmış olduğuna ilişkin kanıtların varlığı teyit edilir. Ön değerlendirme sonuçları ile ilgili olarak Bireysel Bankacılık Müdürü / Bireysel Portföy Yöneticisi (Yönetmeni/Yetkilisi) ve Şube Müdürü'nün bilgilendirildiği ve görüşlerinin alındığı teyit edilir.	25	Banka bünyesinde bireysel kredi başvurusunda bulunan müşteriye ait ön değerlendirme işleminin banka bünyesinde ön değerlendirme işleminden sorumlu olan personel ve/veya personeller tarafından gerekli olan kontrollerin yapılmaması ve buna bağlı olarak ön değerlendirme sonuçlarının yetkili kişilerle paylaşılmaması banka bünyesinde finansal ve operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Çıktıların Gözden geçirilmesi, Mutabakat ve Hataların Ele Alınması	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
2.4	Kredi Başvuru, Değerlendirme Tahsis	MK-OK	Önleyici	Bireysel Krediler	-	Ön değerlendirme sonucu "Red" olan başvurular; kredi girişinin ve "Red" kararının ekran üzerinden yapılması için Bireysel Portföy Yöneticisi (Yetkili/Yetkili Yrd.) tarafından "Dahili Haberleşme Formu" ile Müşteri Hizmetleri Servisi'ne iletilmektedir.	-	İşlem Bazlı	Yıllık	Ön değerlendirme sonucu olumsuz olan kredi başvurularının sisteme giriş süreci incelenir. Denetim dönemi kapsamında "sistem" üzerinden yapılmış olan bireysel kredi başvurularının listesi temin edilir. Ön değerlendirme sonucu "Red" olan başvuru listesinden seçilen örneklem için "Red" kararının, ekran üzerinden girilmesi için Bireysel Portföy Yöneticisi (Yetkili/Yetkili Yrd.) tarafından "Dahili Haberleşme Formu" nun Müşteri Hizmetleri Servisi'ne iletilmiş olduğu teyit edilir.	25	Ön değerlendirme sonucu "red" olan müşterilerin sistem içerisine yetkili olan personeller tarafından tanımlanmaması ve/veya hatalı-yanlış olarak tanımlanması banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Faaliyetleri-Bilgi ve İletişim
2.5	Kredi Başvuru, Değerlendirme Tahsis	MK-OK	Önleyici	Bireysel Krediler	-	Müşteri Hizmetleri Servisi, Operasyon Yetkilisi / Yetkili Yardımcısı tarafından kredi girişi yapılmakta, red gerekçeleri yazılarak (ön değerlendirme sonucu) sistem üzerinden Şube Müdürü'ne yönlendirilmektedir. Şube Müdürü kredi talebinin sistem üzerinden "red" işlemini gerçekleştirmektedir.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında "sistem" üzerinden yapılmış olan bireysel kredi başvurularının listesi alınır. Ön değerlendirme sonucu "Red" olan başvuru listesinden seçilen örneklem için red gerekçelerinin yazılmış olduğu ve Şube Müdürü tarafından sistem üzerinden "red" onayının verildiği teyit edilir.	25	Müşterilere ait bireysel kredi ön değerlendirme sonucuna bağlı olarak, müşteri kredi başvurularının sistem içerisinde yetkili olan ilgili Şube Müdürü tarafından "red" onayının verilmemesi, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir. Sistem içerisinde ön değerlendirme sonucu red edilen müşterilere ait red nedenlerinin etkin ve verimli bir şekilde takip edilmemesi banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyetleri- Bilgi ve İletişim

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
2.6	Kredi Başvuru, Değerlendirme Tahsis	MK	Önleyici	Bireysel Krediler	-	Bireysel Portföy Yöneticisi (Yetkili/Yetkili Yrd) tarafından ön değerlendirmesi başarılı olan kredi başvuruları için, başvuru yapan müşterilerin kendilerinin ve kefillerinin (varsa) başvuru formunda yer alan iş ve ev adreslerini araştırmakta, belirtilen işyerinde çalıştıklarını, ev adreslerinde ikamet ettiklerini, ücretli çalışansa beyan edilen gelirlerinin doğruluğunu teyit etmektedir. İlgili teyitleri yapan personel tarafından belge üzerine "teyit alınmıştır" ibaresi yazılmaktadır.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında "sistem" üzerinden yapılmış olan bireysel kredi başvurularının listesi alınır. Ön değerlendirme sonucu başarılı olan başvurular arasından denetim dönemine yaygın olarak seçilen 25 adet başvuru formu incelenir. Bireysel kredi başvuru formları üzerinde "teyit alınmıştır" ibaresinin varlığı teyit edilir.	25	Ön değerlendirme sonucu "başarılı" olan müşterilere ait bilgilerin banka tarafından teyit edilmemesi, banka bünyesinde operasyonel ve finansal risklerin oluşmasında neden olabilir.	-	Risk Değerlendirme-Kontrol Faaliyetleri
2.7	Kredi Başvuru, Değerlendirme Tahsis	MK-OK	Önleyici	Bireysel Krediler	-	Bireysel Portföy Yöneticisi (Yetkili/Yetkili Yrd) tarafından eksiksiz olan bilgi, belgeler ve istihbarat sonuçları "Dahili Haberleşme Formu" ekinde müşteri kredi talebinin sisteme girişi ve sistem içinden otomatik olarak açılan ekran sorgularının (TCMB, SVT, KKB, Banka varlıkları ve borçları vb.) yapılması için Müşteri Hizmetleri Servisi'ne iletilmektedir.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında "sistem" üzerinden yapılmış olan bireysel kredi başvurularının listesi alınır. Ön değerlendirme sonucu başarılı olan başvurular arasından denetim dönemi itibariyle seçilen 25 adet başvuru için "Dahili Haberleşme Formu" ekinde gerekli bilgi ve belgelerin Müşteri Hizmetleri Servisi'ne iletilmiş olduğu teyit edilir.	25	Müşteri hizmetleri servisi tarafından müşteri kredi talebinin sisteme girişi sırasında otomatik olarak açılan ekranlarda müşteri ile gerekli olan diğer sorgulamaların yapılmaması ve/veya "Dahili Haberleşme Formu"nun ekinde yer alan bilgi ve belgelerin eksik olması nedeniyle gerekli olan sorgulamaların yapılamaması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Risk Değerlendirme-Kontrol Faaliyetleri
2.8	Kredi Başvuru, Değerlendirme Tahsis	MK-OK	Önleyici	Bireysel Krediler	YYY	Müşteri Hizmetleri Servisi, Operasyon Yetkilisi tarafından, kredi başvurusunun YYY sistemine girişi yapılır. Sistem girişini yaparken kesinlikle Şube tarafından yapılan istihbarat sonuçlarının YYY ekranından ilgili alana yazılması gerekmektedir.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında "sistem" üzerinden yapılmış olan bireysel kredi başvurularının listesi temin edilir. Ön değerlendirme sonucu başarılı olan başvurular arasından	25	Sisteme girişi yapılan müşteriye ait kredi başvurusuna ait istihbarat sonuçlarının bulunmaması, müşteri ile ilgili olarak kredi başvurusunun müşteri hizmetleri bölümü tarafından tamamlanamamasına bağlı olarak, banka bünyesinde	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Doğruluk,	Risk Değerlendirme-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										denetim dönemi itibariyle seçilen 25 adet başvuru için YYY sistemi üzerinde Şube tarafından yapılmış olan istihbarat sonuçlarının yer aldığı kontrol edilir. Sistem içerisinde yer alan istihbarat sonuçları alanının YYY Sistemi içerisinde zorunlu alan olarak yer aldığı test edilir.		operasyonel risklerin oluşmasına neden olabilir.	Bütünlük ve Yetkilendirme Kontrolleri	
2.9	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY, TCMB, KKB, SVT, XXX	Bireysel kredi başvuru sahibi ve kefilleri için, YYY sisteminden kredi girişi yapıldıktan sonra sırasıyla kredi akışı sırasında açılan TCMB, KKB, Merkezi Sakınca Veri Tabanı (SVT), XXX Sistemi içerisindeki banka varlıkları (kullanılan kredi, kredi kartı, Destek Hesap, kefil olunan krediler, Banka hesap bilgileri) sorgulamalarının gerekli eşleştirmeler yapılarak araştırılması sağlanmaktadır.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında YYY sistemi üzerinde giriş yapılmış olan bireysel kredi başvuru listesi alınır. Denetim dönemine yaygın olarak seçilen 25 adet örnek üzerinden kredi başvuruları ile ilgili TCMB, KKB, Merkezi Sakınca Veri Tabanı (SVT), XXX Sistemi içerisindeki banka varlıkları (kullanılan kredi, kredi kartı, Destek Hesap, kefil olunan krediler, Banka hesap bilgileri) sorgulamalarının yapılmış olduğu teyit edilir. YYY sistemi üzerinden yapılan sorgulamaların otomatik ve/veya manüel eşleştirme	25	Müşteri tarafından yapılan bireysel kredi başvurusu ile ilgili olarak TCMB, KKB, SVT ve diğer banka varlıklarına ait gerekli olan sorgulamaların yapılmadan kredi başvurusunun banka tarafından değerlendirilip kabul edilmesi banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Risk Değerlendirme- Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										yolu ile yapılıp yapılmadığı sorgulanır. Otomatik yapılan kontrollerle ilgili sistem üzerinde zorunlu işlem kısıtlamasının bulunup bulunmadığı test edilir.				
2.10	Kredi Başvuru, Değerlendirme Tahsis	OK-MK	Önleyici	Bireysel Krediler	XXX	İstihbarat çalışmaları kapsamında, müşteri ve kefillerin ibraz ettiği nüfus cüzdanı bilgilerinin sahte olup olmadığını doğrulamak için KPS (Kimlik Paylaşım Sistemi) sorguları; ibraz edilen adres beyanının sahte olup olmadığının kontrolü için ise XXX "Müşteri Adres Tanımlama" ekranından APS (Adres Paylaşım Sistemi) sorgusu yapılmaktadır.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında YYY sistemi üzerinde giriş yapılmış olan bireysel kredi başvuru listesi alınır. Denetim dönemine kapsamında seçilen 25 adet örnek üzerinden başvuru ile ilgili KPS (Kimlik Paylaşım Sistemi) ve APS (Adres Paylaşım Sistemi) sorgulamalarının yapılmış olduğu teyit edilir.	25	Müşteri tarafından yapılan bireysel kredi başvurusunda yer alan müşteri ve kefillere ait kişisel bilgilerin sorgulanmaması, banka bünyesinde operasyonel, hile ve finansal risklerinin oluşmasına neden olabilir.	Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik	Risk Değerlendirme
2.11	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Bireysel kredi başvurusu için gerçekleştirilmiş olan istihbarat sorguları olumsuz ise, Bireysel Bankacılık Müdürü / Bireysel Portföy Yöneticisi (Yönetmen) ve Şube Müdürü'nün bilgisi dahilinde, kredi talebi YYY sistemi üzerinden Şube Müdürü ekranına gönderilerek, reddedilmesi sağlanmaktadır.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında YYY sistemi üzerinden giriş yapılmış olan bireysel kredi başvuru listesi temin edilir. Liste üzerinde olumsuz istihbarat sonucu olan başvurular seçilir. Oluşan yeni liste üzerinden denetim dönemi kapsamında incelenecek olan örneklem kümesi seçilir. Seçilen örneklem için YYY sistemi üzerinde bulunan başvuru	Test Sırasında Belirlenecek	İstihbarat bilgisi "olumsuz" olarak değerlendirilen müşteriye ait kredi talebinin kontrolsüz bir şekilde onaylanması ve/veya red edilmesi banka bünyesinde finansal ve operasyonel risklere neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Risk Değerlendirme- Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										bilgisinin Şube Müdürü ekranından reddedildiği test edilir.				
2.12	Kredi Başvuru, Değerlendirme Tahsis	MK	Belirleyici	Bireysel Krediler	-	Ön değerlendirmesi ve istihbaratı tamamlanan kredi dosyası Bireysel Bankacılık Müdürü / Bireysel Portföy Yöneticisi (Yönetmen) ve Şube Müdürü'ne sunulur, sistem üzerinden de Şube Müdürü'ne yönlendirilir. Sistem girişi yapıldıktan sonra sistemden alınan "Kredi Talep Formu"; Bireysel Bankacılık Müdürü / Bireysel Portföy Yöneticisi (Yönetmen), Müşteri Hizmetleri Yönetmeni ve Şube Müdürü tarafından kredi dosyasında muhafaza edilmek üzere imzalanmaktadır.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında YYY sistemi üzerinden giriş yapılmış olan bireysel kredi başvuru listesi alınır. Liste üzerinde olumlu istihbarat sonucu olan kredi başvuruları seçilir. Oluşan yeni liste üzerinden denetim dönemi kapsamında örneklem kümesi seçilir. Seçilen örneklem için sistemden alınmış olan "Kredi Talep Formu"nun Bireysel Bankacılık Müdürü / Bireysel Portföy Yöneticisi (Yönetmen), Müşteri Hizmetleri Yönetmeni ve Şube Müdürü tarafından imzalandığı ve kredi dosyasında periyodik olarak muhafaza edildiği kontrol edilir.	Test Sırasında Belirlenecek	Ön değerlendirmesi ve istihbarat işlemleri tanımlanan müşteri kredi dosyasının, banka bünyesinde inceleme ve değerlendirme ile sorumlu olan personel ve/veya bölümlere iletilmemesi ve buna bağlı olarak gerekli onayların alınmadan kredi kullandırımının gerçekleştirilmesi banka bünyesinde finansal ve operasyonel risklerin oluşmasına neden olabilir. İncelemesi tamamlanmış ve ilgili bölüm ve/veya personeller tarafından onaylanmış olan kredi dosyasının banka içerisinde muhafaza edilmemesi banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Kontrol Faaliyetleri-Bilgi ve İletişim
2.13	Kredi Başvuru, Değerlendirme Tahsis	MK	Belirleyici	Bireysel Krediler	YYY	Bireysel Portföy Yöneticisi (Yetkili/Yetkili Yrd.); Bireysel Bankacılık Müdürü / Bireysel Portföy Yöneticisi (Yönetmen), Müşteri Hizmetleri Yönetmeni, Şube Müdürü ile birlikte şube görüşünü oluşturur. Daha sonra "Bireysel Krediler Başvuru Formu"nda ve YYY sistemi içerisinde	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında YYY sistemi üzerinden giriş yapılmış olan bireysel kredi başvuru listesi alınır. Liste üzerinde olumlu istihbarat	Test Sırasında Belirlenecek	Bireysel kredi başvurularında "Şube Görüşü" alanı içerisinde herhangi bir bilginin yer almaması, kredi tahsis işlemi gerçekleştirilecek olan müşteriye ait şube değerlendirmesinin dikkate	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme	Risk Değerlendirme-Bilgi ve İletişim

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						kredi giriş ekranında yer alan "Şube Görüşü Bölümü" doldurulmaktadır.				sonucu olan başvurular filtrelenir. Oluşan yeni liste üzerinden denetim dönemine yaygın olarak tanımlı metodoloji çerçevesinde örneklem seçilir. Seçilen örneklem için "Bireysel Krediler Başvuru Formu"nda ve YYY sistemi üzerinde kredi giriş ekranında yer alan Şube görüşü bölümünün doldurulmuş olduğu teyit edilir.		alınmamasına, buna bağlı olarak banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.		
2.14	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Bireysel Kredi Başvuru talebi eğer şube yetkisinde ise, gerekli imzalar alınmakta ve kredi başvurusu için sistem üzerinden onay verilmektedir. Sistemde şube yetkisi kontrolleri bulunmakta olup, bu kriterlere uymayan talepler; şube yetkisinde onayına izin verilmeksizin, sistem tarafından otomatik olarak Genel Müdürlük bünyesinde yetkili olan personelin ekranına gönderilmektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde tanımlı olan yetki limitleri temin edilir ve incelenir. Şube yetki limiti üzerinde olan bir kredinin YYY sistemi üzerinden otomatik olarak bir üst yetki makamına (Bölge Müdürlüğü, Genel Müdürlük) gönderildiği kontrol edilir. Yapılan kontrollerle ilgili kanıt olarak YYY sistemi üzerindeki ekran görüntüleri alınır.	1	Banka bünyesinde üst yönetim tarafından belirlenmiş olan yetkiler haricinde, bireysel kredi başvurularının yetkili olmayan bölüm ve/veya yetkililer tarafından onaylanması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı-Bilgi ve İletişim
2.15	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Bireysel kredi başvurusu ile ilgili ek analiz gerekiyorsa, Operasyon Yetkili/Yetkili Yrd. Tarafından YYY sistemi üzerinden "Mali Analiz ve istihbarat yapılacaktır" seçeneği seçilir. Bu durumda kredi talebi sistem üzerinden otomatik olarak Bireysel Kredi Analiz Bölümü'ne düşmektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerindeki ilgili ekran içerisinden "Mali Analiz ve istihbarat yapılacaktır" seçeneği seçilir. Ekran üzerindeki	1	Bireysel kredi başvurusu yapılacak olan bir müşteriye ait "Ek Mali Analiz ve İstihbarat" talep edilmesine rağmen, kredi başvuru talebinde bulunan müşteriye banka bünyesinde "Ek Mali Analiz ve İstihbarat"	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyetleri-Bilgi ve İletişim

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										"Tamam" butonuna basıldığı zaman, kredi talebinin otomatik olarak, Bireysel Kredi Analiz Bölümü ekranına düştüğü kontrol edilir. Yapılan kontrollerle ilgili olarak sistem ekran görüntüleri temin edilir.		yapılmaması, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Kaynak Veri Toplama ve Girişi	
2.16	Kredi Başvuru, Değerlendirme Tahsis	MK	Önleyici	Bireysel Krediler	YYY	Ek analiz gerektiren ve Bireysel Kredi Analiz Bölümü'ne yönlendirilen kredilerle ilgili "İstihbarat ve Analiz Raporu" hazırlanmakta ve sistem üzerine kaydedilmektedir.	-	İhtiyaç Bazlı	Yıllık	Denetim dönemi kapsamında YYY sistemi üzerinden ek analiz ihtiyacı doğan bireysel kredi başvuruları ("Mali Analiz ve istihbarat yapılacaktır" seçeneği seçili olanlar) listelenir. Denetim dönemine yaygın olarak, örnekleme metodolojisi kapsamında seçilen örneklem için İstihbarat ve Analiz raporunun hazırlanmış ve sistem üzerine kaydedilmiş olduğu teyit edilir.	Test Sırasında Belirlenecek	Ek analiz gerektiren ve Bireysel Kredi Analiz Bölümü'ne yönlendirilen kredilerle ilgili olarak "İstihbarat ve Analiz Raporu"nun hazırlanmaması ve sistem içerisine kayıt edilmemesi, müşterinin kredi başvurusunun hatalı ve/veya yanlış olarak değerlendirilmesine bağlı olarak banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Bilgi ve İletişim
2.17	Kredi Başvuru, Değerlendirme Tahsis	MK	Önleyici	Bireysel Krediler	YYY	Karar Raporu (kredi başvurusu yapılan tüketici, kefil ve ortaklara ilişkin tüm sorgulamaların sonuçlarına, krediye ilişkin genel bilgilere, belgelere ve kredi ile ilgili ihtiyaç duyulabilecek diğer bilgilere ulaşılan kapsamlı bir rapor) üzerinde kredi onaylanana kadar yapılan tüm adımlar ve adımları gerçekleştiren kişiler, zaman ve açıklamalar yer almakta, bu ekranda kayıt, ekleme, çıkarma vb. işlemler yapılamamaktadır.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde bireysel kredi ile ilgili yapılmış olan işlemlerin kayıt olarak yer aldığı "Karar Raporu" incelenir. Rapor üzerinde manüel olarak değişiklik yapılamadığı kontrol edilir.	1	Müşteri kredi başvuru talebine istinaden yapılan çalışmalar ve buna bağlı olarak verilen onay işlemine ait bilgilerin sistem içerisinde takip edilmemesi ve/veya raporlanmaması banka bünyesinde müşteri kredi başvuru ve onay işlemlerinin etkin ve verimli bir şekilde takip edilememesine bağlı olarak, banka bünyesinde operasyonel ve finansal	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri-	Kontrol Ortamı-Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
												risklerin oluşmasına neden olabilir.	İşlemlerin Yetkilendirilmesi ve Bütünlük	
2.18	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	YYY sistemi üzerine sözleşme dökümü "Sözleşme Ekranı" aracılığıyla yapılmaktadır. Ekran üzerinde yer alan dosya masrafı alanına bilgi girilmeden sistem sürecin işlemesine izin vermemektedir. Sistem içerisindeki masraf alanına ilgili kişi tarafından bilgi girişi yapılmaması durumunda sistem uyarı vermektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerine sözleşme dökümü alınan ekran üzerinde inceleme yapılır. Ekran üzerinde yer alan "dosya masrafı" alanı herhangi bir bilgi girişi yapılmadan boş bırakılarak geçilmeye çalışılır. Yapılan kontrol sonucunda sistemin uyarı verdiği ve işlemin gerçekleştirilemediği teyit edilir.	1	Kredi başvurusu kabul edilen müşteriye ait kredi dosya masrafının, kredi dosyası içerisinde yer almaması ve bununla birlikte müşteriye kredi dosya masrafı alınmadan kredinin tahsis edilmesi, banka gelirlerinin olumsuz yönde etkilenmesine bağlı olarak, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı
2.19	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	YYY sistemi üzerinde bireysel krediler ile ilgili alınacak komisyon ve dosya masrafları sistemde tanımlıdır. Tanımlanmış olan komisyon ve masraf bilgileri ile ilgili olarak sistem içerisinde değişiklik yapılamamaktadır.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde komisyon ve dosya masraflarının tanımlanmasına ilişkin süreç sorgulanır. Sistem üzerinde tanımlanmış olan komisyon ve masrafların kullanıcılar tarafından değiştirilemediği kontrol edilir.	1	Kredi başvurusu kabul edilen müşteriye ait komisyon ve dosya masraflarının müşteri bazında hatalı ve/veya yanlış olarak hesaplanması, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
2.20	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Otomatik değerlendirme sonucu "Red" edilen krediler için YYY sistemi üzerinden gerekli görülen durumlarda "Redde İtiraz" yapılabilmektedir. "Redde İtiraz" komutu kullanıldığında, sistem tarafından karar ekranının açılması sağlanmaktadır. Burada karar seçilip, itiraz için gerekli açıklama yazıldıktan sonra "Tamam" butonu ile kredi talebi otomatik olarak banka Genel Müdürlüğüne gönderilmektedir. Yetkili personel tarafından "red" edilen kredilere ait "redde itiraz" yapılması durumunda sistem tarafından "redde itiraz" işlemi ile ilgili olarak "açıklama bilgisi"nin girilmesi talep edilmelidir. Sistem içerisinde "redde itiraza" ait açıklama alanı zorunlu alan olarak tanımlanmıştır. Sadece sistem üzerinde Genel Müdürlük tarafından redde itiraz tanımı yapılmış olan kredi başvuruları için işlem yapılabilmektedir.	-	İşlem Bazlı	Yıllık	Sistem tarafından yapılan otomatik değerlendirme sonucu "Red" edilen krediler için YYY sistemi üzerinden itiraz yapılması süreci incelenir. Sistem üzerinde, itiraz için gerekli açıklama yazıldıktan sonra "Tamam" komutu ile kredi talebinin otomatik olarak Genel Müdürlüğe gönderildiği teyit edilir. Sistem içerisinde yer alan "Açıklama" alanının "zorunlu" alan olduğu kontrol edilir. Genel Müdürlük tarafından "redde itiraz" tanımı yapılmamış kredi başvurusu için işlem yapılmak istendiğinde sistem tarafından "uyarı" verildiği gözlemlenir.	1	Sistem tarafından otomatik olarak "red edilen" kredi başvurularının, yetkili kişiler tarafından "redde itiraz" yapılmaması, "redde itiraz" yapan yetkili kişi tarafından "redde itiraz" nedeninin sisteme girilmemesi ve "redde itiraz" yapılan kredi başvurularının banka bünyesinde yetkilendirilmiş olan bölüm ve/veya bölümler tarafından değerlendirilmemesi, banka bünyesinde operasyonel risklerin oluşmasına neden olabilir. Redde itiraz yapılmamış olan müşterilere ait sistem tarafından red edilen kredi başvurularının sistem içerisinde yetkisiz olan kişiler tarafından değiştirilebilmesi ve/veya güncellenmesi banka bünyesinde finansal ve operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı Bilgi ve İletişim
2.21	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	YYY sistemi üzerinde iptal edilen krediler için "iptalin kaldırılması" seçeneği mevcuttur. Yetkili personel tarafından sistem içerisinden "İptal Kaldır" komutu verildiğinde "karar" ekranının açılması sağlanmaktadır. Bu alan içerisinde "karar bölümü" seçilip, açıklama yazılarak krediye ait iptal işlemi kaldırılmaktadır. Sistem	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinden iptal edilen krediler için "iptalin kaldırılması" süreci incelenir. "İptal Kaldır" butonuna basıldığında, karar ekranının açıldığı ve bu ekran içerisinde	1	Kredi başvurusu yapan müşterilere ait kredi başvurularının otomatik olarak iptal edilmesi ve iptal edilen kredi başvurularının yetkili ve yetkin olmayan çalışanlar tarafından iptal işleminin banka bünyesinde kabul edilmiş olan standart	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						içerisindeki "Açıklama" alanı zorunlu alandır. Genel Müdürlük tarafından "iptal kaldırma tanımı" yapılmış olan başvuruların iptali kaldırılabilmektedir.				"karar" seçeneğinin seçilip, "açıklama" yazılarak iptal işleminin kaldırıldığı gözlemlenir. Açıklama alanının zorunlu alan olduğu teyit edilir. Sistem üzerinde "iptal kaldırma tanımı" yapılmamış olan kredi başvurusu iptal kaldırma işlemi için sistemin uyarı verdiği gözlemlenir.		uygulamalar dışında gerçekleştirilmesi banka içerisinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	
2.22	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	YYY sistemi üzerinde başvuru yapılan bireysel krediler için krediye ait faiz oranı bilgisi sistem üzerinde tanımlı olan oranlar içerisinden seçilmektedir. Bireysel kredi çeşitleri ve kampanyalar dahilinde sistem üzerinde tanımlanmış olan faiz oranları dışında kredilere ait başka bir oran girilememekte ve sistemdeki faiz oranı değiştirilememektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde başvuru yapılan bireysel kredi tipleri ile ilgili faiz oranı tanımlanması süreci sorgulanır. YYY sistemi üzerinde, bireysel kredi türü ve tanımlanmış kampanyalar dahilinde sistem üzerinde tanımlı olan faiz oranlarının değiştirilemediği kontrol edilir. Sistem üzerinde tanımlı olan faiz oranları dışında müşteriye ait kredi bilgisine manüel olarak faiz oranı bilgisinin girilemediği teyit edilir.	1	Kredi başvurusu yapılan bireysel kredi başvurularına ait kredi faiz oranlarının hatalı ve/veya yanlış olarak belirlenmesi banka bünyesinde kredi kullandırımının hatalı ve/veya yanlış olarak yapılmasına bağlı olarak, banka bünyesinde operasyonel ve finansal risklerin artmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve YetkilendirmeUygulama Kontrolleri-Kaynak Veri Toplama ve GirişiUygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme KontrolleriUygulama Kontrolleri-Veri İşlemede Bütünlük ve GeçerlilikUygulama Kontrolleri-Çıktıların Gözden Geçirilmesi, Mutabakat ve Hataların Ele AlınmasıUygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol OrtamıKontrol Faaliyeti

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
2.23	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Bankaya ait internet sayfası/internet bankacılığı üzerinden kredi başvurusu yapılabilmektedir. İnternet sitesi ve/veya internet bankacılığı üzerinden yapılan başvurular otomatik olarak YYY sistemine aktarılmaktadır. Banka internet sayfası üzerinden yapılan kredi başvurularına ait bilgilerin YYY sistemine tam ve doğru bir şekilde aktarıldığı YYY sistemi tarafından kontrol edilir. Yapılan kontroller sonucunda tespit edilen sorun ve/veya problemler otomatik olarak raporlanır.	-	İşlem Bazlı	Yıllık	Banka internet sayfası/internet bankacılığı üzerinde yer alan bireysel kredi başvuru formu incelenir. Bankaya ait internet sayfası/internet bankacılığı üzerinden doldurulan başvuru formu içerisinde yer alan bilgilerin otomatik olarak YYY sistemine aktarıldığı teyit edilir. YYY Sistemi'ne aktarılamayan ve/veya problemli olan bilgilere ait raporun YYY sistemi tarafından oluşturulduğu kontrol edilir.	1	Banka bünyesinde yer alan kredi başvuru kanallarında yer alan bilgilerin tam ve doğru bir şekilde bankacılık sistemi içerisinde yer almaması ve buna bağlı olarak başvuru kanalları bazında banka bünyesinde yer alan kredi başvuru değerlendirme sürecinin farklılaşması banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı- Bilgi ve İletişim
2.24	Kredi Başvuru, Değerlendirme Tahsis	MK-OK	Önleyici	Bireysel Krediler	-	İnternet sayfası/internet bankacılığı üzerinden yapılan başvurular YYY sistemi üzerinden değerlendirilmek üzere öncelikle GM Bireysel Krediler Grubu'na yönlendirilmektedir. Burada sorgulamalar yapıldıktan sonra yapılan kredi başvurusuna ilişkin değerlendirme sonucu belirlenmektedir. İnternet bankacılığı üzerinden yapılan bir başvuru kapsamında üç farklı karar çıkmaktadır; Onay, Ret, Şubeye Davet. İnternet üzerinden yapılan başvurular kapsamında mutlaka, diğer kredi başvurularında talep edilen bütün belgeler ilgili müşteriden talep edilir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde, arama ekranında "Kanal seçim" kısmında "İnternet" seçilerek, denetim dönemi kapsamında yapılan kredi başvuruları sorgulanır. Kredi tahsis edilen başvurular için, seçilen örneklem kapsamında gerekli dokümanların alınıp alınmadığı kontrol edilir.	Test Sırasında Belirlenecek	Internet veya internet bankacılığı yoluyla yapılan kredi başvurularının banka bünyesinde yetkilendirilmiş bir bölüm tarafından tam, doğru ve zamanında değerlendirilmemesi ve müşteriden bankanın ve ilgili yasal regülasyonun belirtmiş olduğu bilgi ve belgelerin temin edilmemesi banka bünyesinde operayonel, yasal ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme- Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı- Risk Değerlendirme- Kontrol Faaliyetleri-Bilgi ve İletişim
2.25	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Yapılan bireysel kredi başvuruları, YYY sistemi üzerinde yer alan otomatik kredi onay sürecinden geçmektedir. Sistem üzerinde tanımlı yetki limitleri ve tanımlamalar doğrultusunda krediler otomatik olarak onaylanmakta, bir üst	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde tanımlı olan otomatik kredi onay sistemine ait iş akışı incelenir. Süreç içerisinde tanımlı	1	Sistem içerisinde yer alan kredi başvuru onaylarının banka üst yönetimi tarafından onaylanmış ve sisteme tanımlanmış olan yetki ve limit hiyerarşisine uygun	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme Uygulama	Kontrol Ortamı- Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						makama onaya gönderilmekte, "gri alan"a düşmekte veya reddedilmektedir. Gri alana düşen tüm krediler tutar alt limiti olmaksızın Genel Müdürlük Bireysel Krediler Tahsis Bölümü'nün onayına düşmektedir.				olan yetki limitleri ve tanımlamalarının banka bünyesinde onaylanmış ve yayımlanmış olan yetki limitlerini yansıttığı kontrol edilir. Sistem içerisinden "Gri alan"a düşen bireysel kredi başvuru taleplerinin GM Bireysel Kredi Tahsis grubunun onayına düştüğü teyit edilir.		olarak gerçekleştirilmemesi banka bünyesinde kredi tahsis sürecinin etkin ve verimli bir şekilde yürütülememesine bağlı olarak banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Kontrolleri-Kaynak Veri Toplama ve Girişi-Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	
2.26	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Dövize endeksli kredilerde yabancı para kuru Hazine Bölümü tarafından sisteme tanımlanmış olan kur oranlarından otomatik olarak alınmaktadır. Sistemde tanımlı kur oranları şubeler tarafından değiştirilememekte ve ilgili değişiklikler sadece Hazine Bölümü tarafından gerçekleştirilebilmektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerindeki kur oranlarının tanımlanmasına ilişkin süreç incelenir ve sorgulanır. Dövize endeksli kredi işlemlerinde Hazine Bölümü tarafından sisteme tanımlanan yabancı para kurunun şubeler tarafından sistemde tanımlı olan kur bilgilerinden otomatik olarak alındığı teyit edilir. Kullanıcı tarafından sisteme tanımlı olan kur bilgisinin şube tarafından manuel olarak değiştirilemediği test edilir.	1	Dövize endeksli olan kredi başvurularına ait döviz kuru bilgilerinin hatalı ve/veya yanlış olarak dikkate alınmasına bağlı olarak döviz kredisine ait TL tutarının yanlış ve/veya hatalı olarak hesaplanması, banka bünyesinde finansal ve operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi-Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Faaliyeti-Kontrol Ortamı-Bilgi ve İletişim
2.27	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Genel Müdürlük "Bireysel Kredi Tahsis" grubu ekranları üzerinde işlemi giren ve onaylayan mekanizması mevcuttur. İlk değerlendirmeyi birinci Tahsis Yönetmeni, ikinci değerlendirmeyi ikinci Yönetmen ilgili ekran üzerinden yapar. Müşteriye ait	-	İşlem Bazlı	Yıllık	Genel Müdürlük Bireysel Kredi Tahsis grubu ekranları üzerinde girişçi ve onaycı mekanizmasının mevcudiyeti	1	Banka bünyesinde yer alan kredi başvuru, tahsis ve onay işlemlerinin banka üst yönetimi tarafından belirlenmiş ve onaylanmış kurallar kapsamında, ilgili yetkili kişiler tarafından	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyeti

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						kredi tutarı değerlendirmeyi yapan personelin yetkisi dahilindeyse, kredi tutarı onaylanmakta, değilse kredi onayı için Bireysel Kredi Tahsis Müdürünün ve/veya Grup Müdürünün ekranına iletilir.				sorgulanır. Girişçi kullanıcı tarafından kendi girmiş olduğu işleme onay veremediği gözlemlenir. Onaycı kullanıcı tarafından girilen işlem üzerinde değişiklik yapılamadığı, değişiklik yapıldığı durumlarda da başka bir kullanıcının onayına düştüğü kontrol edilir. YYY sistemi üzerinde girişçi ve onaycı mekanizmasının yetki limitleri dahilinde çalıştığı teyit edilir.		yürütülmemesi, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.		
2.28	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	"YYY İş Akışı Giriş" Ekranında "Tamam" komutu verildikten sonra eğer kredi teminatsız bir kredi değil ise "Teminat Bilgileri Giriş" ekranı daima görüntülenmektedir. Ekran üzerinde teminat bilgilerinin girilmesi zorunludur.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde tanımlanmış olan "teminat gerektiren ve gerektirmeyen kredi" bilgileri temin edilir. Temin edilen kredi listesi içerisinden örneklem seçilerek, teminat gerektiren kredilere ait teminat bilgilerinin girişinin YYY sistemine girildiği kontrol edilir. "YYY İş Akışı Giriş" ekranı içerisinde "Tamam" komutu verildikten sonra eğer kredi teminatsız bir kredi değil ise "Teminat Bilgileri Giriş" ekranının görüntülendiği ve	1	Kredi başvurusu yapılmış olan teminatlı bir kredi ile ilgili olarak teminat bilgilerinin temin edilmeden ve teminat bilgilerinin ilgili bankacılık sistemine girilmeden kredi onay işleminin gerçekleştirilmesi, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Faaliyeti

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										ekran üzerinde yer alan bilgileri doldurmadan sistem içerisinde işleme devam edilemediği kontrol edilir.				
2.29	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Bireysel kredi başvuruları sırasında mevduat rehni alınması gerektiği durumlarda, müşteri hesap bakiyesinin müşteri teminat tutarından az olması durumunda başvuru girişine izin verilmekte, sistem sözleşme aşamasında hesap bakiyesinin yeterli olmadığı uyarısı vererek, işleme devam edilmesine izin vermemektedir.	-	İşlem Bazlı	Yıllık	Bireysel kredi başvurusu aşamasında teminat olarak mevduat rehni alınması gerektiği durumlarda hesap bakiyesinin teminat tutarından az olması durumunda banka bünyesinde gerçekleştirilen işlemler incelenir. Sözleşme aşamasında müşteriye ait hesap bakiyesinin yeterli olmadığı durumda YYY Sistemi tarafından müşteri hesap bakiyesinin uygun olmadığına ilişkin uyarı verdiği ve kredi sürecine ait sürecin devam etmediği kontrol edilir.	1	Kredi başvurusunun teminatlı olarak mevduat rehni gerektiren bir kredi türü olmasına rağmen, müşteriden teminat rehninin alınmaması ve/veya müşteriye ait teminat rehni bakiyesinin yeterli olmamasına rağmen banka tarafından müşteriye ilgili kredi tutarının kullandırılması; banka bünyesinde finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyeti
2.30	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Belirli bir müşteri için, Genel Müdürlük Bireysel Krediler Pazarlama Bölümü tarafından belirlenen, Bireysel Tahsis Bölümü tarafından sisteme tanımlanan farklı/özel faiz oranı, gün içerisinde ilgili şube tarafından, ilgili müşteri dışındaki müşterilere uygulanamamaktadır.	-	İhtiyaç Bazlı	Yıllık	Belirli bir müşteri için, Genel Müdürlük Bireysel Krediler Pazarlama Bölümü tarafından özel faiz oranı tanımlanmasına ilişkin süreç sorgulanır. Belirli bir müşteri için tanımlanmış olan özel faiz oranının başka müşteriler için	1	Banka tarafından özel müşterilere uygulanan özel faiz oranlarının kredi başvurusunda bulunan diğer müşterilere de uygulanması ve/veya hatalı bir şekilde uygulanması finansal ve operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Kontrol Faaliyeti

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										kullanılmasının sistem tarafından engellendiği kontrol edilir.				
2.31	Kredi Başvuru, Değerlendirme Tahsis	OK	Önleyici	Bireysel Krediler	YYY	Bireysel kredi başvuruları sırasında sistem üzerinde tanımlı olan limitler kredi türü ve yetki bazında en güncel Yönetim Kurulu kararları doğrultusunda tanımlanmaktadır. Sistem üzerinde tanımlı olan limitler ve tanımlama bilgileri dikkate alınmadan sistem üzerinde kredi başvuru işlemleri onaylanamamakta ve kredi başvuru işlemleri tamamlanamamaktadır.	-	İşlem Bazlı	Yıllık	Bireysel kredi başvuru ve değerlendirme işlemleri ile ilgili olarak en güncel Yönetim Kurulu kararları ve yetki limitleri temin edilir ve incelenir. Sistem üzerinde yapılan tanımlamalar ile Yönetim Kurulu tarafından onaylı olan limit bilgileri ve yetkilendirmeler ile karşılaştırılır. Bankacılık sistemi içerisinde yer alan bilgilerin, sistemin en güncel durumu yansıttığı teyit edilir. Sistem üzerinde tanımlı yetki limitlerinin aşılamadığı test edilir.	1	Bireysel kredi başvuru ve değerlendirme işlemlerinin sistem içerisinde üst yönetim tarafından belirlenmiş olan yetki ve limitler dahilinde yürütülmemesi, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Kontrol Faaliyeti

5.2.3 Kredi Kullandırım Süreci

Kredi kullandırım faaliyeti içerisinde tahsis işlemine ait değerlendirme ve karar adımlarının başarılı bir şekilde gerçekleştirildiğinden emin olduktan sonra, bu işlemlere ait kontrollerin yer aldığı süreçler oluşturulur. Süreçler oluşturulurken, bankanın kullanmış olduğu sistemsel alt yapı, sahip olduğu iş gücü ve bankanın belirlemiş olduğu strateji ve politikalar önem arz eder. Bankaların kullandıkları bilgi sistemleri yapısı, kredilendirme sürecine ait bütün süreçleri (örn. Kredi koşullarının izlenmesi, müşteri teminat bedellerinin kullanım koşulları) kapsayacak şekilde oluşturulur. Kullandırım işlemlerinin regülasyon tarafından belirlenen yasal gereksinimlerin yerine getirilmesi sağlanarak, kredi kullandırımı sağlanır.

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
3	Kredi Kullandırımı					Bireysel kredi kullandırımı süreci kapsamında yer alan kontroller								
3.1	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	YYY sistemi üzerinden bireysel kredi kullandırım ekranları (kredi açılış) üzerinde zorunlu alan kontrolleri mevcuttur.	-	İşlem Bazlı	Yıllık	Bireysel kredi işlemleri kapsamında kullanılan YYY sisteminde kredi kullandırım ekranları (kredi açılış) üzerinde zorunlu alan kontrolleri sorgulanır. Zorunlu alan kontrollerinin çalışıp çalışmadığı teyit edilir.	1	Kredi açılış işlemlerinin hatalı ve/veya yanlış olarak yapılması banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Faaliyeti
3.2	Kredi Kullandırımı	MK	Belirleyici	Bireysel Krediler	-	Taşıt kredileri kullandırılmadan önce Otomotiv Ürünleri Kredi Sözleşmesi, YYY sisteminden alınan Kredi Şartları, Bireysel Krediler Uygulama Esasları dokümanında yer alan gerekli ekler	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinden denetim dönemi kapsamında açılmış olan taşıt kredileri listesi temin edilir. Denetim	25	Taşıt kredileri kullandırım işlemi ile ilgili olarak kredi kullanan müşteriden temin edilmesi gereken bilgi ve belgelerin hatalı ve/veya yanlış olarak temin edilmesi	-	Kontrol Faaliyeti

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						hazırlanmakta; müşteriye ve kefillere (varsa) imzalatılmaktadır.				dönemi kapsamında seçilen 25 adet taşıt kredisi kullandırım işlemi için Otomotiv Ürünleri Kredi Sözleşmesi, YYY sisteminden alınan Kredi Şartları, Bireysel Krediler Uygulama Esasları dokümanında yer alan gerekli eklerin hazırlanmış ve gerekli imzaların alınmış olduğu kontrol edilir.		banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.		
3.3	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	Taşıt kredileri kullandırımı (kredi açılışı) aşamasında YYY sistemi üzerinde şubeleri yönlendirmek için dosya masrafları, varsa komisyon indirgemede kullanılan komisyon bedeli otomatik olarak görüntülenmektedir. Daha sonra bu tutarlar kredi açılışında otomatik olarak kredi tutarından düşülmektedir. Kullanıcıların sistem tarafından hesaplanmış olan tutarlar üzerinde değişiklik yapma yetkileri bulunmamaktadır.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde dosya masrafları ve komisyon oranlarının tanımlı olup olmadığı sorgulanır. Müşteriye kredi açılışı sırasında dosya masrafları ve alınacak komisyon tutarlarının otomatik olarak sistem tarafından hesaplandığı ve hesaplanan tutarlar üzerinde değişiklik yapılamadığı teyit edilir.	1	Müşterilere kullandırılan kredi ile ilgili olarak banka bünyesinde uygulanması gereken banka komisyonu ve dosya masrafı tutarlarının hatalı ve/veya yanlış olarak hesaplanması, bankanın kredilerden elde edeceği ek gelirleri etkileyeceğinden, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Kontrol Faaliyetleri
3.4	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	Taşıt kredileri kullandırımı sırasında dosya ve komisyon masrafları dışında kalan sigorta primi (kasko) masrafları manuel olarak YYY sistemi içerisindeki abc ekranından tahsil edilmektedir. Tahsilat yapılan ekran içerisinde tahsilatı giren ve onaylayan mekanizması mevcuttur.	-	İşlem Bazlı	Yıllık	Taşıt kredileri kullandırımı sırasında, sigorta primi (kasko) masraflarının tahsilat süreci sorgulanır. Sigorta primi masraflarının YYY Sistemi içerisindeki abc ekranından tahsil edildiği ve ekran üzerinde tahsilat bilgisini giren ve	1	Müşteriye kredi kullandırımı aşamasında kasko prim tutarının, kredi kullandırımını sağlayan personel ve/veya bölüm tarafından hatalı ve/veya yanlış hesaplanması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi-Uygulama Kontrolleri-Doğruluk, Bütünlük ve	Kontrol Ortamı-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										tahsilat bilgisini onaylayan mekanizmasının bulunduğu ve ilgili mekanizmanın nasıl çalıştığı incelenir ve sorgulanır.			Yetkilendirme Kontrolleri	
3.5	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	Taşıt kredileri kullandırım aşamasında kullanılan YYY sistemi kredi açılış ekranı üzerinde yer alan tanımlı olan kredi bilgilerinin, kullandırım aşamasında değiştirilmesi durumunda sürecin işlemesine sistem tarafından izin verilmemektedir.	-	İşlem Bazlı	Yıllık	Taşıt kredileri kullandırımı sırasında, YYY sistemi kredi açılış ekranı üzerinde tanımlanmış olan kredi bilgilerinin kullandırım işlemini gerçekleştirilecek olan personel ekranına otomatik olarak geldiği ve söz konusu bilgilerin, kullandırım işlemini gerçekleştirecek olan personel tarafından değiştirilemediği kontrol edilir. Kredi bilgilerinde değişiklik yapılması gerektiğinde, sistem içerisindeki ilgili ekran üzerinde yer alan "Düzelt" komutunun kullanıldığı ve ilgili sürecin YYY sistemi iş akışı üzerinde en başa döndüğü kontrol edilir.	1	Kredi açılış ekranı içerisinde krediyi kullanacak olan müşteriye ait bilgilerin değiştirilmesi ve/veya düzeltilmesine bağlı olarak kredi kullandırımının hatalı ve/veya yanlış olarak gerçekleştirilmesi banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Faaliyetleri
3.6	Kredi Kullandırımı	MK	Önleyici	Bireysel Krediler	-	Ön onayı verilen konut kredileri için Emlak Odası/Derneği Ekspertiz şartları kontrol edilmektedir. Şube Müdürü tarafından, düzenlenen ekspertiz raporu kontrol edilmekte ve imzalanarak işleme alınmaktadır.	-	İşlem Bazlı	Yıllık	Denetim dönemi kapsamında YYY sistemi üzerinden açılmış olan konut kredileri listesi temin edilir. Denetim metodolojisi kapsamında seçilen 25 adet konut kredisi	25	Konut kredisi kullandırım işleminden önce Emlak Odası/Derneği Ekspertiz şartlarının kontrol edilmemesi ve buna bağlı olarak konut kredisinin kullandırılması, banka bünyesinde operasyonel ve finansal	-	Kontrol Ortamı-Kontrol Faaliyeti

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										kullandırım işlemi için düzenlenen ekspertiz raporunun varlığı ve şube müdürü tarafından imzalanmış (onaylanmış) olduğu teyit edilir.		risklerin oluşmasına neden olabilir.		
3.7	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	YYY sistemi üzerinde müşteri tipi ile kredi türünün uyumlu olmasına ilişkin sistemsel kontrol mekanizması mevcuttur (konut kredileri sadece AB, işyeri kredileri {kendi adlarına vergi levhası bulunmayan gerçek kişilerin ve emeklilerin, yeni işyeri (dükkan, büro, muayenehane vb.) alımlarının finanse edilmesi için kullandırılan krediler} ise sadece CD müşteri tipine tanımlıdır).	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde müşteri tipi ve kredi türlerinin uyumlu olmasına ilişkin tasarlanmış kontrollerle ilgili sorgulama yapılır. Konut kredileri için "CD" müşteri tipine kredi açılışı yapılmaya çalışarak, sistem tarafından söz konusu işlemin yapılmasını engellediği test edilir.	1	Müşteri tipine uygun olmayan kredi türlerinin müşterilere tanımlanması, banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Faaliyetleri-Kontrol Ortamı
3.8	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	Ekspertiz/değerleme şirketi tarafından hazırlanan ekspertiz/değerleme rapor ücreti müşteriden YYY Sistemi içerisindeki DEFG ekranı aracılığıyla manüel olarak tahsil edilmektedir. Ekspertiz ve değerleme rapor ücretine ait kullanılan DEFG ekranı üzerinde girişçi ve onaycı mekanizması yer almaktadır.	-	İşlem Bazlı	Yıllık	Ekspertiz/değerleme şirketi tarafından hazırlanan ekspertiz/değerleme rapor ücretinin müşteriden tahsil edilmesine ilişkin süreç sorgulanır. YYY ana bankacılık sistemi üzerinde yer alan DEFG ekranı üzerinde girişçi ve onaycı mekanizmasının varlığı teyit edilir. Söz konusu mekanizmanın tam ve doğru bir şekilde çalıştığı test edilir.	1	Ekspertiz/değerleme şirketi tarafından hazırlanan ekspertiz/değerleme rapor ücretinin müşteriden tahsil edilmemesi ve/veya eksik olarak tahsil edilmesi banka bünyesinde finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme-Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi-Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Faaliyetleri-Kontrol Ortamı

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
3.9	Kredi Kullandırımı	MK	Önleyici	Bireysel Krediler	-	Genel Müdürlük Bireysel Krediler Tahsis Grubu tarafından ön onayı verilen konut kredi talepleri için; SÖBF (Sözleşme Öncesi Bilgi Formu) ve kredi şartları sistemden çıktı olarak alınmakta; müşteri ile varsa kefil/kefillerine imzalatılmaktadır.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinden denetim dönemi kapsamında açılmış olan konut kredileri listesi temin edilir. Denetim metodolojisi kapsamında seçilen 25 adet konut kredisi kullandırım işlemi için SÖBF (Sözleşme Öncesi Bilgi Formu) dokümanının varlığı-sistem ile uygunluğu ve müşteri tarafından (varsa) kefilleri tarafından imzalanmış olduğu kontrol edilir.	25	SÖBF (Sözleşme Öncesi Bilgi Formu) ve kredi şartlarının hatalı ve/veya yanlış bir şekilde oluşturularak müşteriye iletilmesi, müşteri tarafından hatalı ve/veya yanlış formun imzalanması banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Çıktıların Gözden Geçirilmesi, Mutabakat ve Hataların Ele Alınması-Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Faaliyetleri
3.10	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	YYY sistemi üzerinde yer alan SÖBF üzerinde yer alan bilgilerde değişiklik yapıldığı takdirde SÖBF'ün tekrar basılması gerekmektedir. SÖBF üzerinde yer alan bilgilerin bazılarında sistem kontrolü olup, değişiklik sonrası SÖBF'ün tekrar basılmadığı durumda sistemden sözleşme alınması engellenmektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde yer alan SÖBF üzerinde yer alan bilgilerde değişiklik yapıldığı takdirde izlenmesi gereken süreç ile ilgili bilgi alınır. Sistem kontrolü bulunan SÖBF bilgileri sorgulanır ve bu bilgilerde değişiklik yapılarak SÖBF'nin basılmaması durumunda sistemin sözleşme alınmasına izin vermediği teyit edilir.	1	SÖBF (Sözleşme Öncesi Bilgi Formu) içerisinde yer alan bilgilerin değiştirilmesi durumunda söz konusu değişiklik yapılan formun basılmaması ve gerekli değişikliklerin müşteri ile paylaşılmaması banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri-Çıktıların Gözden Geçirilmesi, Mutabakat ve Hataların Ele Alınması	Kontrol Faaliyetleri-Kontrol Ortamı
3.11	Kredi Kullandırımı	MK	Önleyici	Bireysel Krediler	-	Son onayı verilmiş kredi taleplerinde, SÖBF basımını takip eden en erken iki iş günü sonra, taşınmazın bağlı bulunduğu Tapu Sicil Müdürlükleri'nden ilgili ipotek firması tarafından hazırlanan resmi senet ile birlikte taşınmazın "XXX Bank A.Ş. ..... Şubesi" lehine 1.dereceden anapara	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinden denetim dönemi kapsamında açılmış olan konut kredileri listesi temin edilir. Denetim metodolojisi kapsamında seçilen	25	Konut kredisi kullandırımına bağlı olarak banka tarafından konut üzerinde yapılması gereken ipotek işlemlerinin tam, doğru ve zamanında gerçekleştirilmemesi banka bünyesinde operasyonel ve	-	Kontrol Faaliyetleri-Risk Değerlendirme-Kontrol Ortamı

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						ipoteği tesis edilmesi gerekmektedir. Kredi kullandırımından önce söz konusu ipotek belgesinin bulunup bulunmadığı Krediler Bölümü tarafından kontrol edilir.				25 adet konut kredisi kullandırım işlemi için taşınmazın bulunduğu Tapu Sicil Müdürlükleri'nden ilgili ipotek firması tarafından hazırlanan resmi senet ile birlikte taşınmazın "XXX Bank A.Ş. ..... Şubesi" lehine 1.dereceden anapara ipoteği tesis edilmiş olduğu kontrol edilmektedir.		finansal risklerin oluşmasına neden olabilir.		
3.12	Kredi Kullandırımı	MK	Önleyici	Bireysel Krediler	-	Kullandırılacak konut kredisi ile ilgili olarak Bireysel Krediler Uygulama Esasları "Sözleşmelerin Düzenlenmesi" bölümünde anlatıldığı şekilde sözleşme ve eki kredi şartlarını düzenlenmekte ve hazırlanan sözleşme ve kredi şartlarının her sayfası müşteri ve kefil/kefilleri tarafından imzalanmaktadır. Kredi kullandırımı gerçekleştirilmeden önce krediler bölümü tarafından söz konusu işlemlerin yerine getirildiği kontrol edilerek, kredi kullandırımına onay verilir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinden denetim dönemi kapsamında açılmış olan konut kredileri listesi temin edilir. Denetim metodolojisi kapsamında seçilen 25 adet konut kredisi kullandırım işlemi için hazırlanmış olan sözleşme ve kredi şartları dokümanının varlığı ve müşteri ve kefil/kefilleri tarafından imzalanmış olduğu kontrol edilir.	25	Kullandırılan kredi ile ilgili olarak hazırlanan kredi sözleşmesi ve şartları dokümanın müşteri ve/veya müşteri kefilleri tarafından tam, zamanında ve doğru bir şekilde imzalanmaması banka bünyesinde operasyonel, finansal ve yasal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Kontrol Faaliyetleri
3.13	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	Konut kredileri kullandırımı (kredi açılışı) aşamasında YYY sistemi üzerinde şubeleri yönlendirmek için dosya masrafları, varsa komisyon indirgemede kullanılan komisyon bedeli otomatik olarak görüntülenmektedir. Daha sonra bu tutarlar kredi açılışında otomatik olarak kredi tutarından düşülmektedir. Kullanıcıların sistem tarafından hesaplanmış olan tutarlar üzerinde değişiklik yapma yetkileri bulunmamaktadır.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde konut kredilerine ilişkin dosya masrafları ve komisyon oranlarının tanımlı olup olmadığı sorgulanır. Kredi açılışı sırasında dosya masrafları ve alınacak komisyonların otomatik olarak sistem tarafından	1	Konut kredileri ile ilgili olarak kullandırım işlemlerine bağlı olarak dosya masrafları ve komisyon oranlarının hatalı ve/veya yanlış bir şekilde belirlenmesi operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi-Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										hesaplandığı ve hesaplanan tutarlar üzerinde değişiklik yapılamadığı teyit edilir.				
3.14	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	Konut kredileri kullandırımı sırasında dosya ve komisyon masrafları dışında kalan sigorta primi (hayat, konut, DASK) masrafları manuel olarak YYY sistemi üzerinden ABC ekranından tahsil edilmektedir. Ekran üzerinde girişçi ve onaycı mekanizması mevcuttur.	-	İşlem Bazlı	Yıllık	Konut kredileri kullandırımı sırasında, sigorta primi (hayat, konut, DASK) masraflarının tahsilat süreci sorgulanır. Sigorta primi masraflarının YYY sistemi üzerinden ABC ekranından tahsil edildiği ve ekran üzerinde girişçi ve onaycı mekanizmasının varlığı kontrol edilir.	1	Konut kredilerine ait sigorta primi masraflarına ait oluşan tutarların hatalı ve/veya yanlış olarak hesaplanması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri- Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı- Kontrol Faaliyetleri
3.15	Kredi Kullandırımı	MK	Önleyici	Bireysel Krediler	-	İhtiyaç kredileri kullandırımı sırasında, Bireysel Krediler Uygulama Esasları "Sözleşmelerin Düzenlenmesi" bölümünde anlatıldığı şekilde "Kredi Sözleşmesi" ve sistem üzerinden alınan kredi şartları çıktısının her sayfasını müşteri ve kefil/kefilleri tarafından imzalanmaktadır. Kredi sözleşmesi ve kredi şartları çıktısı müşterilere ve kefillere imzalatılmadan kredi kullandırımı gerçekleştirilmemektedir. Kredi sözleşmelerinin ve kredi şartlarının müşteri ve kefiller tarafından imzalandığı kredi kullandırım aşamasından önce Krediler Bölümü tarafından kontrol edilir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinden denetim dönemi kapsamında açılmış olan ihtiyaç kredileri listesi temin edilir. Denetim metodolojisi kapsamında seçilen 25 adet ihtiyaç kredisi kullandırım işlemi için hazırlanmış olan sözleşme ve kredi şartları dokümanının varlığı ve müşteri ve kefil/kefilleri tarafından imzalanmış olduğu kontrol edilir. Sözleşme imzalanma	25	İhtiyaç kredileri kapsamında kullandırılan kredilerle ilgili olarak kredi sözleşmelerinin ve kredi şartlarının müşteriler tarafından tam, doğru ve zamanında imzalanmaması, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı- Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										tarihi ile kredi kullandırım tarihi karşılaştırılır.				
3.16	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	İhtiyaç kredileri kullandırımı sırasında, kredi ile ilgili sigorta, istihbarat ücreti vb. masraflar, YYY ana bankacılık sistemi üzerinde mahsup edildikten sonra kalan kredi tutarı müşterinin hesabına aktarılmaktadır.	-	İşlem Bazlı	Yıllık	İhtiyaç kredileri kullandırımı sırasında masraf ve komisyonların otomatik olarak hesaplanmasına ilişkin süreç sorgulanır. YYY sistemi içerisinde komisyon ve masrafların otomatik olarak mahsup edildikten sonra kalan tutarın ilgili müşteri hesabına yansıdığı kontrol edilir.	1	Kredi kullandırımı sırasında kredi kullanımını gerçekleştiren müşteriye masraflar düşüldükten sonra kalan kredi tutarının hatalı ve/veya yanlış bir şekilde aktarılması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Faaliyetleri
3.17	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	TL cinsinden kullandırılan kredilerde yer alan süreçler ve uygulamalar dövize endeksli kredilerde de aynı şekilde yürütülmektedir. Dövize endeksli kredilerde (DEK) kredi tutarı ilgili döviz cinsinden YYY sistemine girilmektedir. DEK'lerde sözleşme ve açılış tutarlarının birbiriyle aynı olması için Özel Kur Rezervasyonu (ÖKR) alınması zorunludur. ÖKR alınmadan sistem tarafından ilgili müşteriye ait DEK kredi açılışı yapılamamaktadır. Kredi açılışının yapılacağı tarihte ÖKR alınması gerekmektedir.	-	İşlem Bazlı	Yıllık	DEK'lerde sözleşme ve açılış tutarlarının birbiriyle aynı olması için ÖKR alınması süreci sorgulanır. YYY sistemi üzerinde ÖKR alınmadan sistemin işleme izin vermediği teyit edilir. Sistem içerisinde yer alan ÖKR No. alanının zorunlu alan olduğu ve söz konusu bu alanın zorunlu alan olduğu ve sistem tarafından uyarı verildiği test edilir.	1	Dövize endeksli olarak kullandırılan krediye ait sözleşme ve açılış tutarlarının uyumlu olmaması, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
3.18	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	DEK kredi açılış ekranı ilk olarak açıldığında otomatik olarak Serbest Efektif Alış kuru sistem tarafından otomatik olarak getirilmektedir. Sistem içerisindeki otomatik olarak gelen bilgi manüel olarak değiştirilememektedir. ÖKR (özel kur rezervasyonu) girildikten sonra işlem için uygulanacak olan kur bilgisi otomatik olarak güncellenmektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde DEK kredi açılış ekranı üzerinde süreç baştan sona incelenir. Sözleşme ekranı ilk olarak açıldığı sırada otomatik olarak Serbest Efektif Alış kurunun sistem tarafından otomatik olarak getirildiği gözlemlenir. İlgili kurun ÖKR girildikten sonra işlem için uygulanacak kuru gösterecek şekilde otomatik olarak güncellendiği kontrol edilir.	1	Dövize endeksli kredilerde kullanılacak olan döviz kuru bilgisinin bulunmaması ve/veya hatalı-yanlış bir şekilde kullanılması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Faaliyetleri
3.19	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	DEK kredi açılış ekranı üzerinde İstihbarat Dosya Masrafı, Kredi Sigorta Primi, Teminat Sigorta Primi, Ekspertiz Ücreti alanları bireysel kredi türüne göre zorunlu alanlar olup, ilgili tutarlar girilmeden sistem işlemin ilerlemesine izin vermemektedir.	-	İşlem Bazlı	Yıllık	DEK kredi açılış ekranı üzerinde İstihbarat Dosya Masrafı, Kredi Sigorta Primi, Teminat Sigorta Primi, Ekspertiz Ücreti alanları bireysel kredi türüne göre zorunlu alanlar olduğu sorgulanır. İlgili tutar bilgileri girilmeden sistem işlemin ilerlemesine izin vermediği kontrol edilir.	1	DEK kredi türü içerisinde müşteriden tahsil edilmesi gereken masrafların hesaplanmaması ve/veya yanlış hesaplanması, buna bağlı olarak müşteriden hesaplanan ilgili tutarların hatalı ve/veya yanlış bir şekilde tahsil edilmesine neden olabilir. Söz konusu bu durum, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Faaliyetleri
3.20	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	Kredi açılışı yapıldığında dövize endeksli kredi tutarı TL karşılığı müşterinin MT (Türk lirası) hesabına geçer, ayrıca müşteriye nazım hesap bilgisi sistem içerisinde otomatik olarak açılarak, kredi tutarı (kredi para kodu cinsinde) kadar borç kaydedilir. Müşteri tarafından kredi geri ödemesi yapıldıkça, kredi geri ödemesi kadar	-	İşlem Bazlı	Yıllık	Dövize endeksli kredi kullandırımı (kredi açılışı) sonrasında YYY ana bankacılık sistemi üzerinde muhasebe kaydı oluşumuna ilişkin süreç sorgulanır. İşlemin	1	Müşterilere gönderilen dövize endeksli kredi tutarının banka bünyesinde hatalı ve/veya yanlış olarak takip edilmesi ve buna bağlı olarak oluşan muhasebe kayıtlarının hatalı olması banka bünyesinde finansal ve operasyonel	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme-Uygulama Kontrolleri-İşlemlerin	Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						tutar nazım hesaptan anapara tutarı kadar düşülmektedir. İşleme ait muhasebe işlemleri sistem içerisinde otomatik olarak oluşmaktadır.				ilgili muhasebe hesaplarında otomatik olarak kaydedildiği teyit edilir.		risklerin oluşmasına neden olabilir.	Yetkilendirilmesi ve Bütünlük	
3.21	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	YYY sistemi üzerinde bilgiler girilip "Sözleşme" butonuna basıldığında görüntülenen sözleşmede Aylık taksit tutarı, faiz ve diğer bilgilerle birlikte toplam borç tutarı ve ödeme planı kredinin döviz cinsinden otomatik olarak hesaplanmakta ve görüntülenmektedir. Sözleşmede ayrıca kredinin açılış günü TL karşılığı borç tutarı bilgileri de görüntülenmektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde dövize endeksli kredileri için kullandırım sonrası geri ödeme planının oluşum süreci sorgulanır. Kredi açılışı işlemi sonrasında ödeme planının otomatik olarak oluştuğu teyit edilir.	1	Dövize endeksli kredi kullandırımları ile ilgili olarak DEK sözleşmelerinde yer alan kredi borç miktarının ve kredi geri ödeme planının hatalı ve/veya yanlış olarak oluşturulması banka bünyesinde operasyonel, finansal ve yasal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Çıktıların Gözden Geçirilmesi, Mutabakat ve Hataların Ele Alınması	Kontrol Faaliyetleri
3.22	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY	Sistem üzerinde kredi açılışından sonra müşteri hesap değişikliği yapılamamaktadır.	-	İşlem Bazlı	Yıllık	Kredi kullandırım işlemi sonrasında müşteri bilgilerinin değiştirilmesine ilişkin süreç sorgulanır. Sistem üzerinde kredi açılışından sonra müşteri hesap değişikliği yapılıp yapılamadığı test edilir.	1	Kredi kullandırım işlemi sonucunda müşteri hesap bilgilerinin değiştirilmesi banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme	Kontrol Ortamı Kontrol Faaliyetleri
3.23	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY/ XXX	Bireysel krediler kullandırım aşamasında kredi tahsis edilen müşteri hesabından farklı bir müşteri hesabına kullandırım yapılmasına sistem izin vermemektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde kredi tahsis işlemi sırasında sistem üzerinde tanımlı müşteri numarası girilerek limit tahsisi yapıldığı kontrol edilir. Kullandırım aşamasında kullandırım yapılacak hesap bilgisinin kapalı olduğu ve değiştirilemediği teyit edilir.	1	Kredi tahsis edilen müşteriden farklı müşteri hesabına kullandırım yapılması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
3.24	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY/ XXX	Bireysel kredinin kullandırım işlemi (kredi açılışı) sonrasında geri ödeme planı sistem üzerinde otomatik olarak oluşmaktadır.	-	İşlem Bazlı	Yıllık	Kredi kullandırım sonrası ödeme planının oluşturulması süreci sorgulanır. YYY sistemi üzerinden gerçekleştirilen kredi açılışı işlemi sonrasında açılış bilgileri üzerinden geri ödeme planının sistem tarafından otomatik olarak oluşturulduğu kontrol edilir.	1	Kredi açılış işlemi sonrasında kredi geri ödeme planının hatalı ve/veya yanlış olarak hesaplanması, müşteriye hatalı ve yanlış bilgi verilmesinin yanı sıra müşteriden tahsil edilecek olan kredi tahsilatının hatalı ve/veya yanlış takip edilmesine bağlı olarak banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme- Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik	Kontrol Faaliyetleri- İzleme
3.25	Kredi Kullandırımı	OK	Önleyici	Bireysel Krediler	YYY/ XXX	YYY sistemi üzerinden gerçekleştirilen bireysel krediler kullandırım işlemi (kredi açılışı) sonrasında muhasebe işlemleri ana bankacılık sistemi üzerinde otomatik olarak oluşmaktadır.	-	İşlem Bazlı	Yıllık	Bireysel krediler kullandırım işlemlerine ilişkin muhasebe kaydının oluşturulması süreci sorgulanır. Kullandırımı yapılan bireysel kredi türleri için muhasebe kaydının ana bankacılık sistemi üzerinde ilgili hesaplarda sistem tarafından otomatik olarak oluştuğu gözlemlenir. Yapılan kontrollere ilişkin kanıt olarak ekran görüntüleri alınır.	1	Kredi kullandırımına ait oluşan muhasebe işlemlerinin hatalı ve/veya yanlış olarak oluşması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Faaliyetleri
3.26	Kredi Kullandırımı	MK	Belirleyici	Bireysel Krediler	-	Kredi kullandırım işlemleri sonucunda sistem içerisinde oluşan ve çıktısı alınan fişlerin birer nüshası müşteri için açılan "Kredi Dosyası"nda saklanmaktadır. Aslı görülerek fotokopisi ile işlem yapılan evraklardan, nüfus cüzdanı, araç faturası, ruhsat ve tapu dışında kalan evrakların asılları kredi dosyasında muhafaza edilmektedir. Kredi dosyasında muhafaza edilen dokümanlar ilgili bölüm yöneticisi tarafından kontrol edilir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinden denetim dönemi kapsamında açılmış olan konut kredileri listesi temin edilir. Denetim metodolojisi kapsamında seçilen 25 adet konut kredisi kullandırım işlemi için; sistem içerisinden çıktısı	25	Kredi kullandırım işlemlerinin hatalı ve/veya yanlış olarak yapılması ve kredi kullandırımlarında müşteriden alınan ve dosyalanması gereken belge asıllarının müşteri dosyası içerisinde muhafaza edilmemesi banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										alınan fişlerin birer nüshasının ve aslı görülerek fotokopisi ile işlem yapılan evraklardan, nüfus cüzdanı, araç faturası, ruhsat ve tapu dışında kalan evrakların asıllarının kredi dosyasında muhafaza edildiği teyit edilir.				

5.2.4 Kredi Döngüsü-Güncelleme, Tahsilat, İzleme ve Kapama Süreci

Müşteri kredi geri ödemelerinde, müşterinin geçici olarak nakit problemi yaşamasına bağlı olarak kredi ödemelerinde aksaklık yaşayabilir. Bu durumda borçlunun likidite yapısının güçlenmesi buna bağlı olarak kredinin tahsilinin sağlanması için borçluya ait bu krediler yeniden yapılandırılabilir. Yeniden yapılandırma kapsamında borçlu için yeni bir ödeme planı oluşturabilir. Bu işlemlerin gerçekleştirilebilmesi için; borçlunun geri ödeme kabiliyeti kazanacağının iyi belirlenmesi gereklidir. Borçlarını geri ödeme kabiliyeti kazanamayacak olan borçluların finansal yeniden yapılandırma kapsamına alınmaması gereklidir.

Banka bünyesinde krediler sürecine ait oluşturulan kredi izleme ve takip süreçleri, tahsilat süreçlerinin etkinliğini arttırmak amacıyla oluşturularak, söz konusu süreçler içerisinde bu amaç kapsamında gerekli olan kontrol mekanizmaları oluşturulmaktadır.

Kredi miktarının müşteriye tahsisi ile kredi miktarının müşteriden tahsil edilme süresine ait kalan zaman arasında, kredi izleme fonksiyonunda yer alan kontrol faaliyetleri; müşterinin izlenmesi ve kredi ilişkilerinin gözden geçirilmesi faaliyetleri gerçekleştirilir. Kredi izleme faaliyeti, banka tarafından; problemli olan kredilerin çözümü için önlemlerin zamanında alınmasını ön görür. İzleme faaliyeti içerisinde müşterinin kredi sözleşmesi içerisinde bulunan kriterlere uyup uymadığının belirlenmesi işlemleri de yer alır. İzleme faaliyeti, banka sermayesinin regülasyon ve banka içi mevzuata göre yaşanacak olan kayıplar için yeterli olup olmadığı konusunda ön bilgi temin edinilmesini sağlar.

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
4	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)					Bireysel kredilerin tahsilatı, güncellenmesi, kapanması ve izlenmesi süreçleri çerçevesinde yer alan kontrol noktaları								
4.1	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Kullandırılan bireysel krediler için ödeme planı doğrultusunda taksit tahsilatlarında, esas olan, yapılan ödemenin müşterinin kredisinin bağlı olduğu mevduat hesabına alınmasıdır. Müşteri kredisinin bağlı olduğu mevduat hesabı sistem üzerinden değiştirilememektedir.	-	İşlem Bazlı	Yıllık	Banka bünyesinde bireysel kredilere ait geri ödeme işlemleri sorgulanır. Ana bankacılık sistemi üzerinde müşteri kredisinin bağlı bulunduğu mevduat hesabının değiştirilemez olduğu teyit edilir.	1	Kredi tahsisi sağlanan müşteriye ait kredi borcu ve kredi tahsilat bilgilerinin etkin ve verimli bir şekilde takip edilememesi, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik	Kontrol Ortamı Kontrol Faaliyetleri Risk Değerlendirme İzleme
4.2	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Kullandırılan bireysel kredilerde, küçük tutarda eksik yapılan ödemeler veya EFT yoluyla gelen ödemelerde yuvarlama farkları nedeniyle sorun yaşanmaması için sisteme 1 TL tutarına kadar kontrol konulmuş ve 1 TL tutarına kadar gelen eksik ödemelerde tahsilat yapılmakta ve mevduat hesabına kayıt olarak (terse dönmektedir.) işlenmektedir. İşlemle ilgili muhasebe kaydı otomatik olarak sistem tarafından oluşturulmaktadır.	-	İşlem Bazlı	Yıllık	Bireysel kredilerle ilgili olarak banka bünyesinde yürütülen geri ödeme işlemleri sorgulanır. Ana bankacılık sistemi üzerinde küçük tutarda eksik yapılan ödemeler veya EFT yoluyla gelen ödemelerde yuvarlama farkları nedeniyle sorun yaşanmaması için 1 TL' ye kadar gelen eksik ödemelerde tahsilatın yapıldığı ve mevduat hesabının terse döndüğü teyit edilir. İşleme ait muhasebe kaydının otomatik olarak oluştuğu kontrol edilir.	1	Kredi tahsilatlarında oluşan yuvarlama farklılıkları ve eksikliklerin etkin ve verimli bir şekilde takip edilememesi ve bu işlemlere ait muhasebe işlemlerinin hatalı ve/veya eksik olarak gerçekleştirilmesi banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı- Risk Değerlendirme- Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
4.3	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	MK	Belirleyici	Bireysel Krediler	-	Bireysel kredi taksit tahsilatları nedeniyle 1 TL'na kadar terse dönen mevduat hesapları Şubeler tarafından kontrol edilmekte ve "8829990" Nazım hesapla sıfırlanmaktadır.	-	Günlük	Yıllık	Bireysel kredi taksit tahsilatları nedeniyle 1 TL'na kadar terse dönen mevduat hesapları ile ilgili gerçekleştirilen kontroller sorgulanır. Denetim dönemine yaygın olarak seçilen 15 gün için gerçekleştirilen kontrollerle ilgili kanıtların varlığı teyit edilir.	15	Kredi tahsilatlarında oluşan yuvarlama farklılıkları ve eksikliklerin etkin ve verimli bir şekilde takip edilememesi banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı Kontrol Faaliyetleri
4.4	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	MK	Belirleyici	Bireysel Krediler		Bireysel kredi kullanan müşterilerin taksit vadelerinden önce taksitlerini ödemek istediklerini belirtmeleri halinde müşterilere yaptıkları erken ödeme günü oranında faiz indirimi uygulanmaktadır. Müşteriler tarafından yazılı talimat alınarak, erken taksit tahsilat işlemi aynı gün içerisinde yapılmaktadır. Müşterilerden alınan yazılı talimatlar kontrol edilerek, sistem içerisinde gerekli olan bilgi girişleri tamamlanır.	-	İşlem Bazlı	Yıllık	Banka bünyesinde kredi erken taksit tahsilatlarına ait işlemler incelenir. Denetim dönemi kapsamında sistem üzerinden yapılmış olan erken bireysel kredi geri ödeme işlemleri listesi alınır. Denetim dönemine yaygın olarak seçilen 25 adet örnek işlem için yazılı müşteri talimatlarının varlığı sorgulanarak söz konusu tahsilatların aynı gün içerisinde gerçekleştirildiği kontrol edilir.	25	Kredi kullandırımı yapılmış olan müşterilerin kredi taksit bedellerini vadesinden önce bir tarihte ödemesi durumunda banka tarafından uygulanacak olan faiz oranının hatalı ve/veya yanlış olarak belirlenmesi, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Kontrol Faaliyetleri-Bilgi ve İletişim-İzleme
4.5	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Erken geri ödeme işlemleri gerçekleştirilirken taksit tahsilat ekranları üzerinden girilen veriler doğrultusunda yapılacak olan indirim tutarı sistem tarafından otomatik olarak hesaplanmakta ve hesaplanan indirimli tutar bilgisi müşteriden tahsil edilmektedir. Sistem tarafından hesaplanan tutar üzerinde herhangi bir değişiklik yapılamamaktadır.	-	İşlem Bazlı	Yıllık	Müşterilere sağlanan kredilerle ilgili olarak erken taksit tahsilatların gerçekleştirilmesine ilişkin süreç sorgulanır. Erken tahsilat zamanı müşteriye uygulanacak indirim tutarının sistem	1	Kullandırılan krediye ait taksit tutarlarının vadesinden önce tahsil edilmesi durumunda, söz konusu tahsilat işlemlerine ait uygulanacak olan indirim tutarının hatalı ve/veya yanlış olarak hesaplanması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri-Uygulama Kontrolleri-İşlemlerin	Kontrol Ortamı Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										tarafından otomatik olarak hesaplandığı belirlenir. Sistem tarafından hesaplanan tutar üzerinde değişiklik yapılamadığı teyit edilir.			Yetkilendirilmesi ve Bütünlük	
4.6	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Konut Finansmanı Yasası (mortgage) kapsamında kullandırılan kredilerde taksit bedelinin erken ödenmesi halinde, yasa gereği tahsil edilecek tutar üzerinden yasal düzenleme çerçevesinde Banka tarafından kararlaştırılan oran üzerinden erken ödeme ücreti alınmaktadır. Söz konusu erken ödeme ücreti sistem tarafından hesaplamalara dahil edilmekte ve tahsilat işlemi gerçekleştirilmektedir. Sistem tarafından hesaplanan tutar üzerinde değişiklik yapılamamaktadır.	-	İşlem Bazlı	Yıllık	Konut Finansmanı Yasası (mortgage) kapsamında kullandırılan kredilerde taksitin erken ödenmesi halinde yasa gereği tahsil edilecek tutar üzerinden yasal düzenleme çerçevesinde Banka tarafından kararlaştırılan oran üzerinden erken ödeme ücreti alındığı sorgulanır. Söz konusu erken ödeme ücretinin alınması için sistem üzerinde yapılmış olan tanımlama(lar) sorgulanır. Sistem tarafından hesaplanan tutar üzerinde değişiklik yapılamadığı teyit edilir.	1	Konut finansmanı yasası (mortgage) kapsamında kullandırılan kredi miktarına ait erken ödeme yapılması durumunda yasa gereği tahsil edilecek tutar üzerinden yasal düzenleme çerçevesinde banka tarafından kararlaştırılan oran üzerinden erken ödeme ücretinin hatalı ve/veya yanlış olarak alınması banka bünyesinde operasyonel, finansal ve yasal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Risk Değerlendirme Kontrol Faaliyetleri
4.7	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Kullandırılan bireysel krediye ait taksitlerin, taksit tarihinde ödenmemesi halinde, taksit tarihinden ödeme tarihine kadar geçecek günler için, kredi sözleşmesinde belirtilen gecikme faiz oranı baz alınarak gecikme faizi hesaplaması yapılmaktadır. Müşteri taksit ödemesi yapacağında, taksit tutarı ile birlikte gecikme tutarı da tahsil edilmektedir. İlgili	-	İşlem Bazlı	Yıllık	Kullandırılan bireysel krediye ait taksitlerin, taksit tarihinde ödenmemesi halinde gecikme faizlerinin hesaplanması ve müşteriden tahsil edilmesine ilişkin süreç sorgulanır. Sistem tarafından	1	Banka tarafından müşterilere kullandırılan kredilere ait taksit tutarlarının, kredi sözleşmelerinde belirtilen vade tarihinde tam, doğru ve zamanında yatırılıp, yatırılmadığının kontrol edilmemesi ve kredi taksitlerinin vade tarihinde yatırılmaması nedeniyle uygulanacak olan gecikme	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						hesaplamalar sistem tarafından gerçekleştirilmekte ve tutarlar üzerinde değişiklik yapılamamaktadır.				gerçekleştirilen kredi faizi ve gecikme faiz tutarları üzerinde değişiklik yapılamadığı teyit edilir.		faizi tutarının hatalı ve/veya yanlış hesaplanması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.		
4.8	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Kullandırılan bireysel kredi ile ilgili ara ödeme işlemi yapıldıktan sonra kullandırılan krediye ilişkin ödeme planı otomatik olarak güncellenmektedir. *(Ara ödeme, kredi kullanan müşterilerin kredinin herhangi bir döneminde ellerine geçen nakitle taksit tutarlarının düşürülmesi ve ödeyecekleri faiz yükünün azalması amacıyla yapacakları toplu ödemelerdir. Müşterilerin ara ödeme yapabilmeleri için öncelikle geçmiş tarihli taksitlerinden kaynaklanan borçlarının ve masraflarının bulunmaması gerekmektedir.*)	-	İşlem Bazlı	Yıllık	Kullandırılan kredilerle ilgili ara ödeme yapılmasına ilişkin süreç sorgulanır. Ara ödeme işlemi yapıldıktan sonra ödeme planının otomatik olarak güncellenmiş olduğu teyit edilir.	1	Müşterilere kullandırılan kredilere ait gerçekleştirilen ara ödeme işlemlerine ait bilgilerin ödeme planında dikkate alınmaması ve buna bağlı olarak müşteri kredi ödeme planının sistem içerisinde revize edilmemesi, banka bünyesinde müşteriye ait kredi bilgilerinin etkin ve verimli bir şekilde takip edilememesine bu nedenle banka bünyesinde operasyonel ve finansal riskleri oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri-Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyetleri-İzleme
4.9	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	MK	Belirleyici	Bireysel Krediler	-	Ara ödeme işlemi yapıldıktan sonra oluşan yeni geri ödeme planı mutlaka müşteri ve varsa kefil tarafından imzalanmakta ve imzalı ödeme planı kredi dosyasında muhafaza edilmektedir.	-	İşlem Bazlı	Yıllık	Denetim dönemine yaygın olarak sistem üzerinden yapılmış olan ara ödeme yapılmış olan işlemlerin listesi alınır. Denetim metodolojisi gereği seçilen 25 adet örnek ara ödeme işlemi için yeni oluşturulmuş olan ödeme planının müşteri ve varsa kefil/kefillerine imzalatılmış olduğu teyit edilir.	25	Müşteri kredilerine ait ara ödemelere bağlı olarak oluşan yeni ödeme planının müşteri ve kefillere bildirilmemesi ve bildirim sonucunda yeni ödeme planının müşteri ve ilgili kefillere tarafından imzalanmaması banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	-	Kontrol Faaliyeti
4.10	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Kullandırılan bireysel kredi ile ilgili ödeme planında yer alan ödemeler tamamlandıktan sonra müşteriye ait kredi bilgileri sistem üzerinden kapatılmaktadır. Ödeme planında tahsil edilmemiş taksit tutarı kalan kredi hesabı kapatılamamaktadır. Sistem, müşteriye ait kredi	-	İşlem Bazlı	Yıllık	Bireysel kredi kapama işlemi ile ilgili süreç sorgulanır. Süreç üzerindeki kontrol noktalarının varlığı teyit edilir. Ödeme planında yer alan	1	Müşterilere ait kredi tutarının ve/veya kredi taksit tutarlarına ait ödeme (tahsilat) işlemleri gerçekleştirilmeden (tamamlanmadan), sistem içerisindeki yer alan müşteri kredilerinin kapatılması, banka bünyesinde	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme-Uygulama Kontrolleri-Veri İşlemede Bütünlük	Risk Değerlendirme-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						tutarlarının tamamı tamamlanmadan müşteri kredisinin kapatılmasını engeller.				taksitlerin tamamı ödenmeden kredi kapama işlemine sistemin izin vermediği test edilir.		operasyonel ve finansal risklerin oluşmasına neden olabilir.	ve Geçerlilik Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	
4.11	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Bireysel kredi müşterisinin kredisini erken kapatmak istemesi durumunda, kredi kapatma programı tarafından tutar hesaplanmakta, müşteri tarafından ödenen tutar müşterinin kredisinin bağlı olduğu hesaba alınarak kapatma işlemi yapılmaktadır. İşlemlere ait muhasebe kayıtları otomatik olarak oluşmaktadır.	-	İşlem Bazlı	Yıllık	Kullandırılmış olan bireysel kredi işlemleri ile ilgili erken kapatma işlemi gerçekleştirildiğinde banka bünyesinde izlenmesi gereken süreç sorgulanır. Erken kapatma durumunda; müşteri tarafından ödenmesi gereken tutarın sistem üzerinden otomatik olarak hesaplandığı teyit edilir. Gerçekleştirilen işlemlerle ilgili muhasebe kayıtlarının sistem tarafından otomatik olarak oluşturulduğu teyit edilir.	1	Banka müşterilerine ait kredi erken kapatma talebine istinaden erken kapatma tutarının hatalı ve/veya yanlış olarak hesaplanması, müşteri tarafından ödenmesi gereken kredi tutarının hatalı ve/veya yanlış ödenmesine bağlı olarak, banka bünyesinde oluşturulan muhasebe işlemlerinin hatalı oluşmasına, operasyonel ve finansal risklerin ortaya çıkmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Risk Değerlendirme-Kontrol Faaliyetleri-İzleme
4.12	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	MK	Önleyici	Bireysel Krediler	-	Müşteriye ait kredinin vadesinden önce (erken) kapatılması, müşterilerin kredi borcunu vadesinden önce bütünüyle kapatması işlemidir. Kredisini erken kapatmak isteyen müşteriden mutlaka yazılı talimat alınmaktadır.	-	İşlem Bazlı	Yıllık	Denetim dönemine yaygın olarak sistem üzerinden yapılmış olan erken kapama işlem listesi alınır. Denetim metodolojisi gereği seçilen 25 adet örnek erken kapama işlemi için müşteri talimatlarının varlığı teyit edilir.	25	Müşteri talebine istinaden erken ödeme yapılan krediye ait kredi kapama işlemleri ile ilgili olarak müşteriden onaylı bir talimat alınmaması, müşteriye ait erken kapama işlemine ait oluşabilecek olan masrafların müşteriye yansıtılamamasına buna bağlı olarak banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
4.13	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Müşterilerin kredi taksit ödeme tarihlerini değiştirme taleplerinin oluşması durumunda, sistem üzerinde taksit tarihinin değiştirilebilmesi için ertelenmek istenilen gün sayısına karşılık gelen erteleme bedeli otomatik olarak hesaplanmakta ve ilgili tutar müşteriden peşin tahsil edilerek kredinin bağlı olduğu hesaba alınmaktadır. Sistem tarafından hesaplanan tutar üzerinde değişiklik yapılamamaktadır.	-	İşlem Bazlı	Yıllık	Banka bünyesinde müşterilerden gelen taksit erteleme taleplerinin nasıl yürütüldüğü sorgulanır. Sistem üzerinde, taksit tarihinin değiştirilebilmesi için ertelemek istenilen gün sayısına karşılık gelen erteleme bedelinin otomatik olarak hesaplandığı kontrol edilir. Hesaplanan tutar üzerinde değişiklik yapılamadığı teyit edilir.	1	Müşterilerinin kredi taksitleri ile ilgili olarak erteleme taleplerine bağlı olarak oluşan tahsilat kaybının müşteriye yansıtılmaması ve/veya hatalı olarak yansıtılması, banka bünyesinde finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Risk Değerlendirme-Kontrol Faaliyetleri-İzleme
4.14	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Sistemde müşterinin ödemesi gereken toplam BSMV ve KKDF tutarları otomatik olarak hesaplanmakta olup, sistem tarafından yapılan hesaplama üzerinde şubeler tarafından herhangi bir değişiklik yapılamamaktadır.	-	İşlem Bazlı	Yıllık	Banka müşterileri tarafından geri ödenen kredilerle ilgili olarak BSMV ve KKDF tutarlarının hesaplanmasına ilişkin süreç sorgulanır. BSMV ve KKDF tutarlarının sistem tarafından otomatik olarak hesaplandığı ve hesaplanan tutarlar üzerinde sistem tarafından değişikliğe izin verilmediği kontrol edilir.	1	Müşterilerin banka bünyesinden kullanmış oldukları kredilere ait BSMV ve KKDF tutarlarının hatalı ve/veya yanlış olarak hesaplanması, söz konusu tutarların ilgili müşterilerden hatalı ve/veya yanlış tahsil edilmesine bağlı olarak banka bünyesinde finansal ve yasal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı-Kontrol Faaliyetleri
4.15	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Şubelerde taksit ödeme tarihi en fazla 20 gün değiştirilebilir, daha uzun süreli ödeme günü değiştirme talepleri Genel Müdürlük tarafından değerlendirilmektedir. Sistem üzerinde taksit ödeme tarihi 20 günden fazla olacak şekilde gerçekleştirilememektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde taksit ödeme tarihi güncelleme/değiştirme işlemlerinin ne şekilde gerçekleştirildiği sorgulanır. YYY	1	Müşteri kredilerine ait taksit ödeme tarihlerinin yetkisi olmayan kişiler tarafından güncellenmesi ve/veya değiştirilmesi, müşteriye ait taksit ödeme tarihlerinin tam, doğru ve zamanında izlenememesine bağlı olarak,	Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk,	Kontrol Ortamı-Kontrol Faaliyetleri Bilgi ve İletişim

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										sistemi üzerinde ilgili ekranda taksit ödeme tarihi değişikliğinin 20 günden fazla olacak şekilde değiştirilemediği teyit edilir.		banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Bütünlük ve Yetkilendirme Kontrolleri	
4.16	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Otomatik ödeme talimatı belirlenmiş olan bireysel kredi geri ödemeleri için otomatik taksit tahsilat programı çalıştırılmaktadır. Otomatik taksit tahsilat programı çalıştırıldığında ve gün sonu tahsilat işleminde sistem, müşterinin kredi geri ödemesi için tanımlı olan müşteri hesabını kontrol ederek, yeterli bakiye olması halinde tahsilat işlemini gerçekleştirmektedir. İşlemle ilgili muhasebe kayıtları otomatik olarak oluşmaktadır.	-	İşlem Bazlı	Yıllık	Otomatik ödeme talimatı belirlenmiş olan bireysel kredi geri ödemeleri için otomatik taksit tahsilatının ne şekilde gerçekleştirildiği sorgulanır. Otomatik ödemelerin otomatik taksit tahsilat programı aracılığıyla alındığı ve işlemlerle ilgili muhasebe kayıtlarının otomatik olarak oluştuğu teyit edilir.	1	Müşterilere ait kredi taksit tutarlarının tam, doğru ve zamanında tahsil edilmemesi, müşteriden temin edilen tahsilat tutarlarının müşteri kredisine istinaden tahsil edilmemesi ve söz konusu işlemlere ait muhasebe işlemlerinin hatalı ve/veya yanlış olarak gerçekleştirilmesi banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Faaliyetleri- İzleme
4.17	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Belirleyici	Bireysel Krediler	YYY	Kredi taksit ödemelerinin izlenmesi ve ödemelerin zamanında yapılmaması durumunda alınacak olan aksiyonlar, Bireysel Kredi İzleme Grubu koordinasyonunda Şubeler ve Müşteri İletişim Merkezi tarafından yürütülmektedir. Bireysel kredilerde vadesi 90 günü geçen krediler sistem tarafından otomatik olarak takip hesaplarına yansıtılmaktadır.	Bankalarca Karşılık Ayrılacak Kredilerin ve Diğer Alacakların Niteliklerinin Belirlenmesi ve Ayrılacak Karşılıklara İlişkin Esas ve Usuller Hakkında Yönetmelik	İhtiyaç Bazlı	Yıllık	Kredi taksit ödemelerinin izlenmesi ve ödemelerin zamanında yapılmaması durumunda alınacak olan aksiyonlar ile ilgili süreç sorgulanır. Bireysel kredilerde vadesi 90 günü geçen kredilerin sistem tarafından otomatik olarak takip hesaplarına yansıtılmasına ilişkin sistem üzerinde yapılmış olan tasarım teyit edilir. Yapılan tasarımın doğru çalıştığı test edilir.	1	Müşteriler tarafından kredi taksit ödemelerinin tam, doğru ve zamanında yapılmamasına bağlı olarak bu durumun banka tarafından anlık olarak takip edilmemesi, müşteri kredilerine ait geri ödenmeme riskinin artmasına bağlı olarak banka bünyesinde finansal ve yasal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı- Risk Değerlendirme- Kontrol Faaliyeti- İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
4.18	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Krediler takip hesaplarına aktarıldıktan sonra ayrılacak olan karşılık tutarı sistem tarafından otomatik hesaplanmakta ve takip hesapları arasındaki aktarımlar sistem tarafından otomatik olarak yapılmaktadır.	Bankalarca Karşılık Ayrılacak Kredilerin ve Diğer Alacakların Niteliklerinin Belirlenmesi ve Ayrılacak Karşılıklara İlişkin Esas ve Usuller Hakkında Yönetmelik	İhtiyaç Bazlı	Yıllık	Kredi karşılıklarının ayrılmasına ilişkin süreç ve kontroller sorgulanır. Örnek olarak seçilen müşterilere ait kredi karşılık tutarları yeniden hesaplama yöntemi kullanılarak kontrol edilir. Krediler takip hesaplarına aktarıldıktan sonra ayrılacak karşılık tutarlarının sistem tarafından otomatik hesaplandığı ve takip hesapları arasındaki aktarımların yine sistem tarafından otomatik olarak gerçekleştirildiği teyit edilir.	1	Müşterilere kullandırılan ve daha sonra problemli hale gelen kredilere ait banka bünyesinde ayrılması gereken karşılık tutarlarının hatalı ve/veya yanlış olarak ayrılması, banka bünyesinde finansal ve yasal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik- Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Risk Değerlendirme- Kontrol Faaliyetleri
4.19	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK-MK	Önleyici	Bireysel Krediler	YYY	İhtarname gönderilerek takip sürecine alınacak tüm kredilerle ilgili karar Bireysel Kredi İzleme Grubu tarafından verilerek şubelere bildirilmektedir. Kredilerle ilgili hesap özeti ve ihtar mektupları sistemden otomatik olarak alınmakta olup, kredi sözleşmesinde bulunan bilgiler ile ihtarname üzerine yazılan bilgilerin aynı olduğu şube personeli tarafından kontrol edilmektedir. Sistem üzerinde kredi ile ilgili bilgiler bu aşamada kullanıcılar tarafından değiştirilememektedir.	-	İhtiyaç Bazlı	Yıllık	İhtarname gönderilerek takip sürecine alınacak kredilerle ilgili süreç sorgulanır. Kredilerle ilgili hesap özeti ve ihtar mektuplarının sistemden otomatik olarak alındığı ve bu bilgiler üzerinde değişiklik yapılamadığı teyit edilir.	1	Kredi görünümlerinde problem olan müşterilere ait banka bünyesinde alınması gereken aksiyonların yetkili ve yetkin bir bölüm tarafından gerçekleştirilmemesi ve buna bağlı olarak, müşteri ile ilgili olarak yürütülecek olan ihtarname sürecinin hatalı ve/veya yanlış yürütülmesi, banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri- Çıktıların Gözden Geçirilmesi, Mutabakat ve Hataların Ele Alınması	Kontrol Ortamı- Risk Değerlendirme- Kontrol Faaliyetleri- Bilgi ve İletişim
4.20	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY/ XXX	İhtarname gönderilmesi aşamasına gelen müşterilerin banka genelinde başka kredisi / kredileri bulunması halinde, diğer kredileri için de ihtarname gönderilerek müşteri kredilerinin kesintiye uğraması sağlanmaktadır. İlgili işlem sistem	-	İhtiyaç Bazlı	Yıllık	İhtarname gönderilmesi aşamasına gelen müşterilerin Banka genelinde başka kredisi / kredileri bulunması halinde,	1	Banka bünyesinde izlenen ve değerlendirilen kredi müşterilerinden, ihtarname aşamasında bulunan bir müşteriye ait diğer kredi bilgilerinin ihtarname sürecinde dikkate alınmaması,	Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri Uygulama	Kontrol Ortamı- Risk Değerlendirme- Kontrol Faaliyetleri- İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						tarafından otomatik olarak yapılmakta ve müşteri risk takip programı aracılığıyla müşterinin diğer kredileri de kesintiye uğratılmaktadır.				diğer kredileri için de ihtarname gönderilerek kredilerin kesintiye uğratılması süreci sorgulanır. Müşteri Risk Takip programı ve sistem üzerinde bu kapsamda yapılan tanımlamalar sorgulanır ve etkinliği test edilir.		müşteriye ait diğer kredilerle ilgili olarak ihtar işlemlerinin uygulanamamasına bağlı olarak banka bünyesinde finansal risklerin oluşmasına neden olabilir.	Kontrolleri-İşlemlerin Yetkilendirilmesi ve Bütünlük	
4.21	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Teminat grubu ve alınan teminat değişikliği kredi açılışından en az bir gün sonra yapılabilmektedir. Teminat grubu ve alınan teminatlarla ilgili değişiklik, düzeltme, teminat eklenmesi ya da teminat çıkışı YYY sistemi ekranlarından yapılmaktadır. Teminatlarla ilgili değişiklik Genel Müdürlük onayı gerektiriyorsa (tanımlı olan parametrelere göre) sistem krediyi otomatik olarak Genel Müdürlüğe göndermekte daha sonra şube onayına düşmektedir. Genel Müdürlük tarafından onaylanan değişikliğe şube onay verdikten sonra etkin hale gelmektedir.	-	İhtiyaç Bazlı	Yıllık	YYY sistemi üzerinde kredi açılış günü teminat grubu ve alınan teminatlara ilişkin değişiklik yapılması süreci incelenir ve test edilir. Sistem içerisinde gerçekleştirilen teminat değişikliği ve/veya güncellemesi ile ilgili olarak sistem tarafından yapılan kontrollerin ve engellemelerin tam ve doğru bir şekilde çalıştığı test edilir. Girilen teminat ile ilgili GM onayı tanımlı ise, ilgili işlemin sistem üzerinden GM birimlerine düştüğü gözlemlenir. Gerekli onaylar sonrasında sistem içerisinde kayıtların oluştuğu teyit edilir.	1	Kredi açılış işleminden sonra müşteriden alınan teminat türlerinin ve tutarlarının yetkili olmayan bölüm ve/veya personel tarafından sistem içerisinde değiştirilmesi ve söz konusu bu değişikliklerin yönetim tarafından onaylanmış olan kurallar dahilinde yapılmaması, banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri-Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	Kontrol Ortamı-Kontrol Faaliyetleri-Bilgi ve İletişim

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
4.22	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	MK	Belirleyici	Bireysel Krediler	YYY	Bankada kullandırılan kredilerin teminatlarının (ipotek, rehin, mevduat v.b.) çözülmesi ancak banka alacağının fer'ileriyle birlikte tamamen tasfiyesiyle mümkündür. Bu nedenle, şubeler riskin tamamen tasfiye olduğunu bildirerek ve ödenmemiş olan her türlü masrafları (örn: sigorta prim borcu, ihbarname masrafları vb.) öncelikle tahsil ederek, ipoteğin, taşıt rehninin kaldırılmasına veya benzeri bir başka teminatın çözülmesine dair talepleri mail ile Bireysel Kredi İzleme Grubu'nun onayına sunmaktadır. Bireysel Kredi İzleme Grubu talepleri inceler ve incelenen taleplere istinaden sorun olmayan müşteri kredilerini onaylar.	-	İşlem Bazlı	Yıllık	Bankada kullandırılan kredilerin teminatlarının çözülmesine ilişkin süreç sorgulanır. Teminatlı olarak kullandırılan bireysel krediler kapsamında, denetim dönemine yaygın olarak sistem üzerinden kapanmış krediler listesi alınır. Denetim metodolojisine uygun olarak, seçilen 25 adet örnek üzerinde teminatların çözülmesine dair e-maillerin gönderildiği, gerekli evrakların alındığı/hazırlandığı ve gerekli onayların alınmış olduğu teyit edilir.	25	Banka tarafından müşteri kredilerine istinaden alınan teminatların çözülme işleminin hatalı ve/veya yanlış bir şekilde yapılması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyetleri-Bilgi ve İletişim
4.23	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	OK	Önleyici	Bireysel Krediler	YYY	Bireysel kredilerde teminata alınan mevduat blokelerinin çözümü gerekli şartlar sağlandıktan sonra sistem içerisinde yer alan girişçi ve onaycı mekanizması dahilinde gerçekleştirilmektedir.	-	İşlem Bazlı	Yıllık	Bireysel kredilerde teminat olarak alınan mevduat blokelerinin girişçi ve onaycı mekanizması dahilinde gerçekleştirildiği teyit edilir.	1	Kredi kullandırım işlemine istinaden müşterilerden teminat olarak alınan mevduat blokelerinin banka bünyesinde ne şekilde, hangi kurallar dahilinde ve hangi sorumlu bölüm tarafından çözümlendirilmesi gerektiğinin belirlenmemesi, operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyetleri
4.24	Kredi Döngüsü (Güncelleme, Tahsilat, İzleme, Kapama)	MK-OK	Belirleyici-Önleyici	İç Kontrol	YYY	Bireysel kredilerle ilgili reeskont hesaplamaları otomatik olarak sistem tarafından hesaplanmaktadır. Aylık olarak İç Kontrol birimleri tarafından sistemden hesaplanan Reeskont tutarlarının örnekleme kontrolü ve Reeskont-Mizan mutabakatı ve kontrolü gerçekleştirilmektedir.	-	Aylık	Yıllık	Bireysel kredilerle ilgili reeskont hesaplamalarının sistem tarafından otomatik olarak hesaplandığı teyit edilir. İç Kontrol birimleri tarafından	2	Müşterilere kullandırılan kredilere ait reeskont hesaplamalarının sistem tarafından hatalı ve/veya yanlış olarak hesaplanması finansal tablolarda yer alan reeskont bedelinin hatalı ve/veya yanlış yer almasına	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri-Çıktıların Gözden Geçirilmesi,	Kontrol Ortamı-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										sistemden hesaplanan Reeskont tutarlarının örnekleme kontrolü, Reeskont-Mizan mutabakatı ve kontrolü çalışmalarının; denetim dönemine yaygın olarak denetim metodolojisi gereği seçilen 2 ay için gerçekleştirilmiş olduğu doğrulanır.		bağlı olarak banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Mutabakat ve Hataların Ele Alınması	
4.25	Kredi Döngüsü (Güncelleme, Tahsilat, Kapama, İzleme)	OK	Önleyici	Bireysel Krediler	YYY	YYY ana bankacılık uygulamasında bireysel kredi kullandırım ve geri ödeme işlemleri sonrasında tek düzen hesap planına uygun muhasebe hareketleri sistem tarafından otomatik olarak oluşmaktadır.	-	İşlem Bazlı	Yıllık	YYY ana bankacılık uygulaması üzerinde bireysel kredi kullandırım ve geri ödeme işlemleri sonrasında oluşan muhasebe işlemlerine ait muhasebe kayıtlarının sistem içerisinde nasıl oluştuğu sorgulanır. Seçilen örneklere istinaden ilgili örnekler kapsamında muhasebe hareketlerinin sistem tarafından doğru bir şekilde otomatik olarak oluşturulduğu teyit edilir.	1	Kredi kullandırım ve geri ödeme işlemlerine istinaden oluşan muhasebe kayıtlarına ait bilgilerin muhasebe sistemi içerisinde hatalı ve/veya yanlış şekilde oluşturulması, operasyonel, finansal ve yasal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik	Kontrol Faaliyetleri

5.2.5 Kredi Yakın İzleme ve Kanuni Takip Süreci

Banka bünyesinde oluşturulan portföyler içerisinde yer alan kredi ve borç bilgilerinin durumunun sürekli olarak izlenmesi ve analiz edilmesi ile ilgili olarak, banka bünyesinde stratejik hedeflerle ve regülasyonun ön gördüğü kriterler çerçevesinde prosedürler geliştirilir ve uygulanır. Oluşturulan prosedürler kapsamında uygulanan faaliyetler içerisinde, kredi ve alacakların daha yakından ve izlenme sıklığının artmasına bağlı olarak farklı bir kredi sınıfından tanımlanmasına, ilgili müşteriye ait karşılık uygulamasının gerçekleştirilmesi veya ek olarak bazı düzeltici tedbirlerin oluşturulmasına neden olan sorunlu kredilerin tespit edilmesine ve söz konusu bu işlemlerin nasıl, ne zaman ve kime raporlanacağına ilişkin standartlar oluşturulur.

Kredi anlaşması sonucunda belirlenmiş olan geri ödeme anlaşmasının önemli ölçüde bozulduğu ve/veya bozulması ön görülen anapara ve faiz ödemelerinde gecikmelerin yaşandığı ve dolayısıyla da zarar olasılığının belirdiği kredilerle ilgili olarak banka bünyesinde yakın izleme ve/veya kanuni takip süreci yürütülmektedir. Bankaların sorunlu kredilere ait yakın izleme ve kanuni takip sürecini tam, doğru ve zamanında gerçekleştirmemesi bankalar bünyesinde;

1) Sorunlu olarak ortaya çıkacak olan kredilere ait sağlanan fonların daha fazla getiri getiren diğer alanlara yönlendirilmemesine,

2) Problemli olan kredilerin daha yakın takip edilmesine bağlı olarak banka bünyesindeki idari giderlerin artmasına,

3) Söz konusu kredilerle ilgili banka bünyesinde yer alan yöneticilerin ilgi ve zamanını daha verimli alanlarda değerlendirilememesine neden olabilir.

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
5	Yakın İzleme ve Kanuni Takip					Yakın izleme ve kanuni takipte yer alan krediler ile ilgili kontroller								
5.1	Yakın İzleme ve Kanuni Takip	OK	Belirleyici	Bireysel Krediler	-	Bireysel Kredilerin kanuni takip hesaplarına aktarım sürecinin entegrasyonu yürürlüğe konulmuş olan YYY sistemine tanımlı Müşteri Bazlı Risk Takip programı ile sağlanmaktadır. Müşteri Risk Takip Raporu ile herhangi bir hesabı takibe atılmış olan müşteri saptanarak, var olan başka bir hesabı var ise takip aktarılması yapılır. Müşteri Risk Takip Raporuna ek olarak, takip hesaplarına aktarımlarla ilgili sistem üzerinde tanımlanmış kişilere günlük olarak otomatik e-mail gönderilmektedir.	-	Günlük	Yıllık	Müşteri bazlı risk takip programının faaliyeti ve gerçekleştirmiş olduğu işlemlerle ilgili olarak inceleme gerçekleştirilir ve ilgili programda yapılan bilgi tanımlamalarının güncelliği kontrol edilir. Takip hesaplarına otomatik aktarımlara ilişkin ilgili kişilerin/birimlerin bilgilendirilmesine dair sistem üzerindeki tanım (otomatik e-mail) incelenir ve test edilir.	1	Banka bünyesinde herhangi bir hesabı takibe alınmış olan müşteriye ait diğer hesapların takibe alınmaması ve söz konusu takip işlemi ile ilgili olarak banka bünyesinde yer alan ilgili bölümlere bilgi verilmemesi, operasyonel, yasal ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik Uygulama Kontrolleri- İşlemlerin Yetkilendirilmesi ve Bütünlük	Kontrol Ortamı- Risk Değerlendirme- Kontrol Faaliyetleri- Bilgi ve İletişim
5.2	Yakın İzleme ve Kanuni Takip	OK	Önleyici	Bireysel Krediler	YYY	Müşteriye ihtarname çekildikten sonra müşteri tarafından ödeme yapılmamışsa, 91. gün sonunda ilgili kredi sistem tarafından otomatik olarak yasal takip hesabına aktarılmaktadır. Müşteri tarafından 91. gün içerisinde ödeme yapılması durumunda, sistem tarafından oluşturulan fişin iptal işlemi İzleme Grubu tarafından yapılabilir. Kredinin Yasal takip hesaplarına aktarımdan sonra sistem tarafından gün sayılarak otomatik olarak karşılık hesaplanıp, gerekli kayıtlar sistem içerisinde oluşturulmaktadır.	Bankalarca Karşılık Ayrılacak Kredilerin ve Diğer Alacakların Niteliklerinin Belirlenmesi ve Ayrılacak Karşılıklara İlişkin Esas ve Usuller Hakkında Yönetmelik	İşlem Bazlı	Yıllık	Yasal takip süreçlerine ilişkin sistem üzerinde yapılmış olan tanımlamalar gözden geçirilir. Güncel durumun mevzuatla uyumlu olduğu teyit edilir. Banka bünyesinde tasarlanmış olan yapının etkin çalıştığı test edilir.	1	Regülasyon tarafından, karşılık ayrılacak olan kredilerin belirlenmesi ve karşılık ayrılmasına ilişkin oluşturulmuş olan kural(lar) bütününe banka bünyesinde uyulmaması ve/veya hatalı, yanlış bir şekilde uygulanması ve söz konusu işlemlere ait muhasebe kayıtlarının tam, doğru ve zamanında gerçekleştirilmemesi operasyonel, finansal ve yasal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik	Risk Değerlendirme- Kontrol Faaliyetleri- İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
5.3	Yakın İzleme ve Kanuni Takip	OK	Önleyici	Bireysel Krediler	YYY	Yasal takibe tabi tutulan (atılan) müşterilere atanan statü kodları ile YYY sistemi tarafından müşterinin varlık hesapları bloke edilmektedir. Takip hesaplarında bakiyesi olan müşterilerin mevduat hesaplarında bakiye kalmaması gerektiğinden, mahsup işlemi yapılıncaya kadar hesap borç kaydına kapatılmaktadır.	-	İşlem Bazlı	Yıllık	Yasal takip süreci kapsamında müşterinin varlık hesaplarının ne şekilde bloke edildiğine ilişkin süreç sorgulanır. YYY sistemi üzerinde yasal takibe atılan müşterilere ait varlıkların otomatik olarak bloke edilmesine ilişkin test işlemleri gerçekleştirilir.	1	Yasal takip başlatılan ve sistem içerisinde yasal takipte olan müşteriler kategorisinde takip edilen müşterilere ait mevduat hesaplarının bloke edilmemesi, mevduat hesaplarında yer alan tutarın takipteki müşteriler tarafından alınmasına neden olabilir. Bu durum banka bünyesinde finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri- Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik	Risk Değerlendirme- Kontrol Faaliyetleri-İzleme
5.4	Yakın İzleme ve Kanuni Takip	MK	Belirleyici	İç Kontrol	YYY	Takipteki kredilerde izlenen tüm müşterilerin YYY sistemi üzerinde başka aktif bir kredisi olup olmadığı sistem içerisinden çekilen raporlarla haftalık olarak kontrol edilmektedir.	-	Haftalık	Yıllık	Takipteki kredilerde izlenen tüm müşterilerin YYY sistemi üzerinde canlı kredisi olup olmadığına ilişkin İç Kontrol birimleri tarafından yapılan haftalık incelemede sorgulanır. Denetim dönemine yaygın olarak seçilen 5 hafta için ilgili kontrolün yapılmış olduğu teyit edilir.	5	Banka bünyesinde yer alan ve takipte olan müşterilere ait "aktif" durumda olan kredi bilgisinin bulunması ve söz konusu kredilerin sistem içerisinde takip pozisyonunda tanımlanmaması operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Kontrol Faaliyetleri-İzleme
5.5	Yakın İzleme ve Kanuni Takip	MK	Belirleyici	İç Kontrol	-	Takipteki kredilerde izlenen müşteriye ait aktif durumda olan izlenen KMH kredisinin bulunup bulunmadığına sistem içerisinden temin edilen raporlarla haftalık olarak kontrol edilir.	-	Haftalık	Yıllık	Takipteki kredilerde izlenen tüm müşterilerin aktif durumda olan ve izlenen KMH kredisi olup olmadığı ile ilgili olarak İç Kontrol birimleri tarafından yapılan haftalık incelemeler sorgulanır. Denetim dönemine yaygın olarak seçilen 5 hafta için ilgili kontrolün yapılmış olduğu teyit edilir.	5	Banka bünyesinde yer alan ve takipte olan müşterilere ait "aktif" durumda olan KMH bilgisinin bulunması ve söz konusu kredilerin sistem içerisinde takip pozisyonunda tanımlanmaması operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Kontrol Faaliyetleri İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
5.6	Yakın İzleme ve Kanuni Takip	MK	Belirleyici	İç Kontrol	-	Kanuni takibe aktarılmış olan müşterilerin mevduat hesaplarına bloke işleminin uygulanmaması veya kanuni takipte olan müşterinin hesabına gelen tutarların tahsil edildiği 4 ayda bir İç Kontrol birimleri tarafından gerekli olan kontrol işlemleri gerçekleştirilir.	-	Dört Aylık	Yıllık	Kanuni takibe aktarılmış olan müşterilerin mevduat hesaplarına bloke işleminin uygulanmaması veya müşteri hesabına gelen tutarların tahsil edilmemesi ile ilgili olarak gerçekleştirilen işlemler hakkında bilgi temin edilir ve süreç içerisinde gerçekleştirilen faaliyetler sorgulanır. Denetim dönemine yaygın olarak 2 dönem (dört aylık periyot) için İç Kontrol birimleri tarafından ilgili süreç içerisinde gerçekleştirilen kontrollerin periyodik olarak gerçekleştirildiği kontrol edilir.	2	Banka bünyesinde kanuni takip işlemi uygulanan müşterilere ait mevduat hesapları için bloke işleminin uygulanmaması ve buna bağlı olarak müşteri mevduat hesabına yatırılan tutarların takip işlemine istinaden tahsilat işlemi olarak dikkate alınmaması, operasyonel ve finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyeti İzleme
5.7	Yakın İzleme ve Kanuni Takip	MK	Belirleyici	Bireysel Krediler	-	Kanuni takibe intikal ettirilecek krediler için; • Kredi sözleşmesinin/sözleşmelerini (Avukat tarafından istenmesi durumunda aslı) • Borçlunun, kefillerin, kimlik ve ikametgâh bilgileri • Kredi teminatlarının dökümü ve teminatlarla ilgili belgeler • Bireysel Kredi İzleme Grubu'ndan alınan teyit doğrultusunda kredi kesilme tarihi itibariyle mevcut risk anapara, faiz, temerrüt faizi ve ferileri toplamı dökümü • Müşteriye gönderilmiş olan tebliğ	-	İşlem Bazlı	Yıllık	Kanuni takibe intikal ettirilecek krediler için nasıl bir süreç izlendiği sorgulanır. Kanuni takip yapılması amacıyla Hukuk Bölümü'ne hangi belgelerin gönderildiği sorgulanır. Denetim dönemi itibariyle kanuni takibe düşen bireysel kredi listesi sistem üzerinden temin edilir. Denetim metodolojisi kapsamında seçilen 25 adet örnek kredi	25	Kanuni takibe intikal ettirilecek olan kredi bilgilerine istinaden Hukuk Bölümü tarafından kanuni takip başlatılması için gerekli olan bilgi ve belgelerin Hukuk Bölümü'ne tam, doğru ve eksiksiz bir şekilde iletilmesi operasyonel ve yasal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Risk Değerlendirme-Kontrol Faaliyetleri-Bilgi ve İletişim-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
						şerhli ihtarname • Yapılan malvarlığı araştırması sonucunda elde edilen bilgiler hazırlanarak eksiksiz bir biçimde Hukuk Bölümü'ne gönderilmektedir.				için hazırlanması gerekli evrakların hazırlanmış ve eksiksiz bir şekilde Hukuk Bölümü'ne gönderilmiş olduğu teyit edilir.				

5.2.6 Kredi Süreci İle İlgili Olan Yetki ve Parametre İşlemleri

Krediler sürecine ait gerçekleştirilen uygulama ve kontroller içerisinde kullanılan bilgi sistemleri alt yapı teknolojisinin karmaşıklığı ve/veya çeşitliliği, söz konusu sistem ve/veya sistemler içerisinde işlem yapan kullanıcılara ait yetki tanımlamalarının periyodik olarak gözden geçirilmesini ortaya çıkarmaktadır. Bunun yanında, krediler kapsamında banka bünyesinde uygulanan operasyonlara ait parametre kriterlerinin yasal regülasyon kapsamında belirlenen standartlara ve banka yönetimine ait stratejilerle uygun hale getirilmelidir. Tanımlanan parametrelerin periyodik olarak kontrol edilmesi banka bünyesinde gerçekleştirilen kredi sürecinin etkinliğini ve verimliliğini arttıracaktır. Kredi işlemlerini yürüten organizasyonun yapısı işlevsel olmalıdır. Organizasyon yapısında görev ayrımı sağlamalı ve yetki çatışması oluşmamalıdır. Oluşturulan yapının periyodik olarak kontrol edilmesi sağlanmalıdır.

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
6	Yetkiler ve Parametre İşlemleri					Bireysel Krediler Süreci kapsamında incelenen ekranlara erişim yetkileri ile kritik parametre değişikliklerinin gerçekleştirildiği ekranlar üzerindeki kontroller								
6.1	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	XXX	XXX uygulamasında kullanıcı yaratma ve yetkilendirme işlemleri, görevler ayrılığı prensibine uygun olarak bir başka kullanıcının onayına tabidir. Yetkilendirme işlemleri, kullanıcıların görev tanımlarına göre oluşturulmuş standart yetki tanımları dahilinde gerçekleştirilmektedir.	Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ	İşlem Bazlı	Yıllık	XXX uygulamasında kullanıcı yaratma, kullanıcı yetkilendirme ve profil yetkilerini değiştirme işlemleri ayrı ayrı incelenir. İşlemlerin gerçekleşmeden önce onaya tabi olduğu, giriş yapan kullanıcıların kendi girdikleri işlemleri onaylayamadıkları ve onay sırasında girişi yapılan bilgiler	1	Bankacılık sistemi içerisinde yer alan krediler süreci ile ilişkili olan uygulamalar içerisindeki; kullanıcı yaratma, yetkilendirme ve kullanıcı profillerini değiştirme işlemlerinin belirli kurallar ve yetkilendirmeler dahilinde kontrol altına alıp yönetilmemesi, krediler süreci ile ilgili olarak uygulamaların yetkisiz kişiler tarafından hatalı ve/veya yanlış bir şekilde gerçekleştirilmesine neden olmakla birlikte bu durum operasyonel ve yasal	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı-Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										üzerinde değişiklik yapılamadığı teyit edilir. Reddedilen işlemlerin gerçekleşmediği kontrol edilir. Ayrıca, hangi profilin hangi yetkilere sahip olması ve hangi kullanıcının hangi yetki grubuna atanması gerektiğine yönelik standart dokümanlar oluşturulmuş olması ve yetkilerin periyodik olarak bu standartlar ile karşılaştırılması beklenmektedir. İstisnai yetki taleplerinin ne şekilde gerçekleştirileceği de bu standartlar ile belirlenmiş olmalıdır. Yapılan kontrollere ilişkin kanıt olarak ekran görüntüleri temin edilir.		risklerin oluşmasına neden olabilir.		
6.2	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	Bireysel krediler uygulaması olan YYY sistemi üzerinde kullanıcı yaratma ve yetkilendirme işlemleri, görevler ayrılığı prensibine uygun olarak bir başka kullanıcının onayına tabidir. Yetkilendirme işlemleri, kullanıcıların görev tanımlarına göre oluşturulmuş standart yetki tanımları dahilinde gerçekleştirilmektedir.	Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ	İşlem Bazlı	Yıllık	YYY uygulaması üzerinde kullanıcı yaratma, kullanıcı yetkilendirme ve profil yetkilerini değiştirme işlemleri ayrı ayrı incelenir. İşlemlerin gerçekleşmeden önce onaya tabi olduğu, giriş yapan kullanıcıların kendi girdikleri işlemleri onaylayamadıkları	1	Bireysel krediler uygulamasının banka yönetimi tarafından belirlenmiş olan yetkili ve yetkin personel tarafından kullanılmaması ve ilgili uygulama içerisinde yer alan (oluşturulan) yetki hiyerarşisinin etkin ve verimli bir şekilde kullanılmaması, operasyonel ve yasal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı-Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										ve onay sırasında girişi yapılan bilgiler üzerinde değişiklik yapılamadığı teyit edilir. Reddedilen işlemlerin gerçekleşmediği test edilir. Ayrıca, hangi profilin hangi yetkilere sahip olması ve hangi kullanıcının hangi yetki paketine atanması gerektiğine yönelik standart dokümanlar oluşturulmuş olması ve yetkilerin periyodik olarak bu standartlar ile karşılaştırılması beklenmektedir. İstisnai yetki taleplerinin ne şekilde gerçekleştirileceği de bu standartlar ile belirlenmiş olmalıdır. Yapılan kontrollere ilişkin kanıt olarak ekran görüntüleri temin edilir.				
6.3	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	Bireysel krediler uygulaması olan YYY sistemi üzerinde onay yetkileri (şube) kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda bulunmaktadır.	-	İşlem Bazlı	Yıllık	YYY uygulaması üzerinde, bireysel krediler ile ilgili kritik onayların verildiği onay ekranına erişim listesi incelenir. Sadece görev tanımı gereği erişimi bulunması gereken kişilerin ekrana eriştikleri teyit edilir.	Tüm Popülasyon	Krediler süreci içerisinde görev alan banka personeline ait görev tanımları ile sistem içerisinde yer alan rollerinin ve yetki tanımlamalarının uyumlu olmaması, krediler sürecine ait işlemlerin etkin ve verimli yürütülmemesine bağlı olarak operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
6.4	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	YYY sistemi üzerinde yer alan şube-bölge-Genel Müdürlük yetkilerinin, limitlerinin tanımlanması ve değişikliği girişçi ve onaycı mekanizması doğrultusunda yapılmaktadır.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde yer alan şube-bölge-Genel Müdürlük yetkilerinin ve limitlerinin tanımlanması süreci sorgulanır. İlgili yetkilerin ve limitlerin girişçi ve onaycı mekanizması dahilinde yapıldığı teyit edilir.	Tüm Popülasyon	Banka bünyesinde bireysel kredi süreci içerisinde yer alan bölüm ve/veya lokasyonlara ait görev ve sorumlulukların sistem içerisinde ayrıştırılmaması, banka bünyesinde operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi	Kontrol Ortamı Kontrol Faaliyeti
6.5	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	Kredi Açılış Ekranı üzerinde kredi açılış bilgileri ile ilgili değişiklik yapma yetkileri ("Düzelt" butonu) kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda bulunmaktadır.	-	İşlem Bazlı	Yıllık	Kredi Açılış Ekranı üzerinde kredi açılış bilgileri ile ilgili değişiklik yapma yetkileri ("Düzelt" butonu) sorgulanır. Sadece görev tanımı gereği erişimi bulunması gereken kişilerin ekrana eriştikleri ve yetki sahibi olduğu kontrol edilir.	Tüm Popülasyon	Kredi açılış ekranı içerisindeki değişiklik yapma yetkisinin, yetkisi olmayan kullanıcılar tarafından kullanılması, operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi	Kontrol Ortamı- Kontrol Faaliyetleri
6.6	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	Otomatik değerlendirme sonucu "Red" edilen krediler için YYY sistemi üzerinden gerekli görülen durumlarda "Redde İtiraz" yapılabilmektedir. Burada karar seçilip, itiraz için gerekli açıklama yazıldıktan sonra "Tamam" butonu ile kredi Genel Müdürlüğe gönderilebilmektedir. Redde itiraz yetkisi sadece onay yetkisine sahip kullanıcılarda mevcuttur. Genel Müdürlüğün izin vermediği durumlarda butona basıldığında sistem tarafından uyarı verilmektedir.	-	İşlem Bazlı	Yıllık	Otomatik değerlendirme sonucu "Red" edilen krediler için YYY sistemi üzerinden gerekli görülen durumlarda "Redde İtiraz" yapılmasına imkân tanıyan yetkiler sorgulanır. Redde itiraz yetkisinin sadece onay yetkisine sahip kullanıcılarda mevcut olduğu teyit edilir. Genel Müdürlüğün izin vermediği durumlarda redde itiraz butonuna	Tüm Popülasyon	Sistem tarafından otomatik olarak "red edilen" kredi başvuruları ile ilgili olarak sistem tarafından otomatik işleyen süreç içerisinde redde itiraz işlem yetkisinin banka bünyesinde yetkili olan kişilere tanımlanmaması ve/veya söz konusu işlem yetkisinin kredi sürecinde rol alan her personel tarafından kullanılabilmesi, operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik	Kontrol Ortamı- Kontrol Faaliyetleri-Bilgi ve İletişim

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										basıldığında sistem tarafından uyarı verildiği gözlemlenir.				
6.7	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	YYY sistemi üzerinde iptal edilen krediler için iptalin kaldırılması seçeneği mevcuttur. "İptal Kaldır" butonuna basıldığında karar ekranının açılması sağlanmaktadır. Burada "karar" seçeneği seçilip, açıklama yazılarak iptal işlemi kaldırılmaktadır. Açıklama alanı zorunlu alandır. İptal kaldırma yetkisi sadece onay yetkisine sahip kullanıcılarda mevcuttur. Genel Müdürlüğün izin vermediği durumlarda butona basıldığında sistem tarafından uyarı verilmektedir.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde iptal edilen krediler için iptalin kaldırılmasına imkân tanıyan yetkiler sorgulanır. İptal kaldırma yetkisinin sadece onay yetkisine sahip kullanıcılarda mevcut olduğu teyit edilir. Genel Müdürlüğün izin vermediği durumlarda iptal kaldır butonuna basıldığında sistem tarafından uyarı verildiği gözlemlenir.	Tüm Popülasyon	Sistem içerisinde çeşitli nedenlerden dolayı iptal edilmiş olan bir krediye ait "iptal kaldırma" işlem yetkisinin, banka bünyesinde söz konusu operasyonel yetkiye sahip olmayan bir kullanıcı tarafından kullanılması, operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme-Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi-Uygulama Kontrolleri- Veri İşlemede Bütünlük ve Geçerlilik	Kontrol Ortamı-Kontrol Faaliyetleri
6.8	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	YYY sistemi üzerinde tanımlı parametrelerin ve iş akışının yönetildiği "Genel Kriter Ekranı"na erişim yetkileri kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda bulunmaktadır.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde tanımlı parametrelerin, limit tanımlamalarının ve iş akışının yönetildiği "Genel Kriter Ekranı"na erişim yetkileri sorgulanır. Erişim yetkilerinin kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda (Bireysel Krediler Ürün ve Süreç Geliştirme) bulunduğu teyit edilir.	Tüm Popülasyon	Banka sistemi içerisinde kredi sürecinin yürütüldüğü modül ve/veya programa ait parametrelerin yer aldığı "Genel Kriterler Ekranı"na yetkili olmayan kullanıcıların erişim yetkilerinin bulunması, operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
6.9	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	YYY sistemi üzerinde tanımlı parametrelerin ve iş akışının yönetildiği "Genel Kriter Ekranı" üzerinde girişçi ve onaycı mekanizması mevcuttur.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde tanımlı parametrelerin, limit tanımlamalarının ve iş akışının yönetildiği "Genel Kriter Ekranı"na erişim yetkileri sorgulanır. Ekran üzerinde girişçi ve onaycı mekanizmasının tesis edilmiş olduğu test edilir.	1	Krediler sürecinin yürütüldüğü sistem içerisinde yer alan "Genel Kriter Ekranı" içerisine tanımlanan parametrelerin hatalı ve/veya yanlış tanımlanması, krediler süreci içerisinde oluşturulan işlemlerin hatalı ve/veya yanlış oluşturulmasına bağlı olarak operasyonel risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı-Kontrol Faaliyetleri
6.10	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	Bireysel kredi kampanya tanımlarının yapıldığı "Kampanya Tanımlama Ekranları"na erişim yetkileri kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda bulunmaktadır.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde kampanya tanımlarının yapıldığı "Kampanya Tanımlama Ekranları"na erişim yetkileri sorgulanır. Erişim yetkilerinin kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda (Bireysel Krediler Pazarlama, Tahsis) bulunduğu teyit edilir.	Tüm Popülasyon	Bireysel kredilere ait kampanya tanımlamalarının yapıldığı ekranların yetkisiz kişiler tarafından kullanılması operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı-Kontrol Faaliyetleri
6.11	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	Bireysel kredi kampanya tanımlarının yapıldığı "Kampanya Tanımlama Ekranları" üzerinde girişçi ve onaycı mekanizması mevcuttur.	-	İşlem Bazlı	Yıllık	YYY sistemi üzerinde kampanya tanımlarının yapıldığı "Kampanya Tanımlama Ekranları"na erişim yetkileri sorgulanır. Ekran üzerinde girişçi ve onaycı mekanizmasının tesis edilmiş olduğu test edilir.	1	Bireysel kredilere ait kampanya tanımlamalarının hatalı ve/veya yanlış bir şekilde yapılması banka bünyesinde operasyonel ve finansal risklerin oluşmasına neden olabilir.	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve YetkilendirmeUygulama Kontrolleri-Kaynak Veri Toplama ve Girişi	Kontrol Ortamı-Kontrol Faaliyetleri
6.12	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	Bireysel Kredilere ilişkin ödeme süresi değiştirme ekranına (vadeyi uzatmak ya da kısaltmak) erişim yetkileri kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda bulunmaktadır.	-	İşlem Bazlı	Yıllık	Bireysel Kredilere ilişkin ödeme süresi değiştirme ekranına (vadeyi uzatmak ya da kısaltmak) erişim yetkileri sorgulanır.	Tüm Popülasyon	Bireysel krediler süreci içerisinde yer alan kredi ödeme süresi ile ilgili olarak yapılan değişiklik işleminin banka bünyesinde yetkilendirilmemesi, kredi	Uygulama Kontrolleri-Kaynak Veri Hazırlama ve YetkilendirmeUygulama Kontrolleri-	Kontrol Ortamı-Kontrol Faaliyetleri

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										Erişim yetkilerinin kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda (Bireysel Kredi İzleme - Ödeme İşlemleri Grubu) bulunduğu teyit edilir.		ödeme süresi ile ilgili olarak yapılan değişiklikliklerin takip edilmemesine bağlı olarak operasyonel ve finansal risklerin oluşmasına neden olabilir.	Kaynak Veri Toplama ve Girişi	
6.13	Yetkiler ve Parametre İşlemleri	OK	Önleyici	BT	YYY	Sistem üzerinde kanuni takip hesaplarına otomatik olarak aktarılamayan kredilerin manüel olarak takip hesaplarına aktarımlarının yapıldığı (örn. KMH) "Aktarım Ekranı"na erişim yetkileri kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda bulunmaktadır.	-	İşlem Bazlı	Yıllık	Sistem üzerinde kanuni takip hesaplarına otomatik olarak aktarılamayan kredilerin manüel olarak takip hesaplarına aktarımlarının yapıldığı (örn. KMH) "Aktarım Ekranı"na erişim yetkileri sorgulanır. Erişim yetkilerinin kullanıcıların görev tanımlarına uygun olarak kısıtlı sayıda çalışanda (Bireysel Kredi İzleme) bulunduğu teyit edilir.	Tüm Popülasyon	Sistem tarafından takip hesaplarına otomatik olarak aktarılamayan kredilerin, manuel olarak aktarılması işleminin yetkisiz olan personel tarafından yapılması, operasyonel ve finansal risklere neden olabilir.	Uygulama Kontrolleri- Kaynak Veri Hazırlama ve Yetkilendirme Uygulama Kontrolleri- Kaynak Veri Toplama ve Girişi	Kontrol Ortamı- Kontrol Faaliyetleri

5.2.7 Kredi Süreci İçerisindeki İç Kontrol İşlemleri

Bankanın karşılaştığı kredi riskini kontrol altına almanın en etkin yolu kredilendirme süreç kontrolüdür. Krediler sürecine ait iç kontrol kapsamında kredi işlemlerindeki ana ve alt süreçlere ait sorunların giderilmesi operasyonel risklerin minimize edilmesini temin etmekle birlikte, regülasyonun ön gördüğü kural ve kriterlere bağlı olarak karşılaşılması muhtemel görünen risklerin kontrol edilmesini sağlar. Kontrol faaliyetleri sonucunda yaşanan risk ve sonuçları yeniden gözden geçirilmelidir. Kontrol işlemleri tarafsız bir şekilde değerlendirilerek, etkin bir kontrol ve izleme yapılarak kontrol edilen sürecin sonuçları değerlendirilmelidir.

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
7	İç Kontrol					Bireysel Krediler süreci üzerinde İç Kontrol birimleri tarafından gerçekleştirilen kontroller								
7.1	İç Kontrol	MK	Belirleyici	İç Kontrol	YYY	YYY Sistemi içerisindeki "ABC" ekranlarından teminata alınan döviz kodları ile risklerin döviz cinsleri ve taksitler toplamları kontrol edilmektedir.	-	Altı Aylık	Yıllık	Teminatı mevduat rehni olan kredilerde, ek ve farklı türde bir teminat alınmadığı sürece, mevduat rehni tutarı ile kredi risk tutarı aynı para cinsi ise mevduat rehni tutarının kredi taksitler toplamından az olup olmadığı kontrol edilmektedir. Teminatı mevduat rehni olan DEK'lerde, ek ve farklı türde bir teminat alınmadığı sürece, teminat farklı döviz cinsi ise karşı parite ile değerlenmiş tutarın kredi taksitler toplamından az olup olmadığı kontrol	1	Müşteriye kullandırılan kredilerle ilgili olarak müşterilerden alınan teminat bedellerinin, regülasyon tarafından ve/veya banka yönetimi tarafından belirlenen limit aralığında olmaması, finansal ve yasal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
										edilmektedir. TL krediye uygun görülen cinsteki (USD, EUR, GBP, CHF) YP mevduat rehni alınması durumunda YP mevduatın para cinsi üzerinden ve taksitler toplamının sözleşme tarihindeki TCMB Döviz Alış Kuru ile karşılığının %110'u kadar olmaması kontrol edilmektedir. DEK'lere TL mevduat rehni alınması durumunda TL üzerinden ve taksitler toplamı üzerinden sözleşme tarihindeki TCMB Döviz Alış Kuru ile karşılığı TL'nin %120'si kadar olmaması kontrol edilmektedir. İlgili kontrolün yapılmış olduğu seçilen bir dönem (6 aylık periyot) için teyit edilir.				
7.2	İç Kontrol	MK	Belirleyici	İç Kontrol	YYY	YYY Sistemi içerisindeki "DEF" ekranı vasıtasıyla 90 günden uzun süre faizi sıfırlanmayan KMH hesapları belirlenerek Risk İzleme Bölümü'nden açıklama istenmektedir.	-	Aylık	Yıllık	Denetim dönemi kapsamında, seçilen 2 ay için İç Kontrol birimleri tarafından 90 günden uzun süre faizi sıfırlanmayan Kredili Mevduat Hesaplarının kontrolünün yapıldığına ilişkin test işlemi gerçekleştirilir.	2	Müşterilere tanımlanmış ancak uzun süredir kullanılmayan KMH hesaplarına ait faiz bilgisinin sıfırlanmaması finansal ve operasyonel risklere neden olabilir.	-	Kontrol Ortamı-Risk Değerlendirme Kontrol Faaliyetleri-İzleme

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
7.3	İç Kontrol	MK	Belirleyici	İç Kontrol	YYY	Vade bilgisi +90 gün geçtiği halde Kanuni Takip hesaplarına aktarılmayan Bireysel kredi olup olmadığı günlük olarak kontrol edilmektedir.	-	Günlük	Yıllık	Denetim dönemi kapsamında, seçilen 15 gün için İç Kontrol birimleri tarafından vade bilgisi +90 gün geçtiği halde Kanuni Takip hesaplarına aktarılmayan Bireysel kredi olup olmadığına ilişkin kontrol işleminin yapıldığı test edilir.	15	Ödeme vade bilgisi +90 gün üzerinde olan kredi bilgilerinin kanuni takip hesaplarına aktarılmaması, finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Risk Değerlendirme Kontrol Faaliyetleri-İzleme
7.4	İç Kontrol	MK	Belirleyici	İç Kontrol	YYY	Bireysel krediler ile ilgili aylık olarak reeskont ve mizan mutabakatı yapılmaktadır.	-	Aylık	Yıllık	Denetim dönemi kapsamında, seçilen 2 ay için İç Kontrol birimleri tarafından aylık olarak reeskont mizan mutabakatı yapıldığına ilişkin kanıt temin edilir.	2	Kredilere ait reeskont tutarlarının hatalı ve/veya yanlış bir şekilde hesaplanması buna bağlı olarak banka finansal tablolarında yer alan reeskont tutarının hatalı ve/veya yanlış bir şekilde yer almasına neden olabilir. Bu durum finansal risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı-Kontrol Faaliyetleri

5.2.8 Kredi Süreci İçerisindeki Genel Kontroller

No	Alt Süreç	Kontrol Tipi	Kontrol Türü	Kontrol Sahibi	Sistem	Kontrol Tanımı	İlgili Regülasyon	Kontrol Sıklığı	Test Sıklığı	Test Yöntemi	Test Örnek Sayısı	Risk	COBIT Referans	COSO Bileşeni
8	Genel					Bireysel Krediler süreci üzerindeki kontrol noktalarının güncelliği								
8.1	Genel	MK	Belirleyici	Bireysel Krediler	-	Bireysel krediler süreci üzerindeki kontrol noktalarının güncelliği ve geçerliliği Bireysel Krediler Grubu tarafından yıllık olarak gözden geçirilir.	-	Yıllık	Yıllık	Bireysel krediler süreci üzerindeki kontrol noktalarının güncelliğinin ve geçerliliğinin güvence altına alınabilmesi için kontrol listelerinin süreç sahipleri tarafından teyit edildiği; sistem ve prosedür değişiklikleri takip edilerek gerektiğinde kontrollerin güncellendiği gözlemlenir.	1	Banka bünyesinde yürütülen kredi işlemlerine ait operasyonların kontrol noktalarının periyodik olarak gözden geçirilmemesi ve/veya güncellenmemesi, operasyonel risklerin oluşmasına neden olabilir.	-	Kontrol Ortamı- Risk Değerlendirme- Kontrol Faaliyetleri- İzleme

SONUÇ

Çalışma kapsamında COBIT (uygulama ve genel kontrolleri) ve COSO modeli kapsamında yer alan kontrollerin işletme bünyesinde yürütülen işlemlerle bağlantısının bulunup bulunmadığı araştırılmıştır. Yapılan ön çalışmalarda yerel yasal mevzuatın desteği nedeniyle COBIT standartlarının en çok bankacılık sektöründe uygulanabilir durumda olması, bankacılık sektörü kapsamında yer alan süreçlerin incelenmesine kaynak oluşturmuştur. Yabancı ortaklı bankaların, uygulama anlamında daha fazla kaynağa sahip olduğu, ancak sektör bünyesinde yer alan diğer bankaların bu kaynaktan yoksun oldukları görülmektedir.

Temelde tüm bankalar için büyüklük, organizasyonel yapıya bağlı olarak bireysel krediler sürecinde faklılıklar bulunmasına rağmen; bankalar bünyesinde benzer olarak yürütülen süreçlerden biri olması nedeniyle bireysel krediler süreci tercih edilmiştir. Böylece çalışmanın sektör temsilcilerinin tümü için anlaşılabilir ve uyarlanabilir bir uygulama örneği olması amaçlanmıştır. Bunun yanında bireysel kredi süreci farklı sektörlerden temsilciler tarafından da değerlendirilebileceği ve konuya yakın olacağı için uygulamanın farklı alanlar içerisinde uygulanmasının daha uygun olacağı düşünülmüştür.

Yapılan çalışma sonucunda bankalarda yürütülen bireysel krediler süreci içerisinde yer alan risklere ait kontrol faaliyetlerinin genel olarak;

- COBIT **uygulama kontrolleri** ile bağlantılarının kurulabildiği tespit edilmiş olup,

- **Genel kontrollere** ait bağlantıların DS- Hizmet Sunumu ve Destek, AI- Tedarik ve Uygulama ve ME- İzleme ve Değerlendirme kapsamında kurulabildiği görülmüştür.

Daha güvenli bir kontrol ortamı kurulabilmesi için; banka bünyesinde oluşturulan stratejik hedef ve planlamalar doğrultusunda yürütülen bireysel krediler sürecine ait faaliyetlerde yer alan kontrol mekanizmalarının ve erken uyarı mekanizmalarını oluşturulan süreç ve alt süreçlerinin dizaynı ve tasarımında COBIT

uygulama kontrollerinin ve COSO kontrollerinin dikkate alınabileceğini ortaya koymuştur.

Uygulama örneğinde oluşturulan risk kontrol matrisi incelendiğinde, bankacılık operasyonlarından önemli biri olan bireysel krediler süreci içerisinde yürütülen faaliyetler için karşılaşılması muhtemel risk tanımlamaları yapılmış ve söz konusu bu risk tanımlamalarına karşılık gelen kontrol faaliyetleri açıklanmıştır. Çalışma içerisinde; bankalar bünyesinde gerçekleştirilen kontrollerin manuel ve/veya otomatik olabildiği, söz konusu yürütülen işlemlere ait bilgi sistemi risklerinin birçoğunun bilgi sistemlerinden kaynaklanmadığı; söz konusu risklerin manuel olarak yürütülen işlemler neticesinde oluşabildiği sonucuna varılmıştır. Süreçler kapsamında risklerini ve kontrol noktalarını belirleyen ve teknolojik gelişmelere bağlı olarak risk ve kontrollerini güncelleyen bankalar, risklerini minimize etmek istediği noktalara bilgi teknolojileri yatırımlarını kaydırarak, manuel riskleri insan kaynağı yatırımları ya da farklı süreç dizaynları yolu ile azaltmayı deneyebilecektir.

Operasyonel süreçler içerisinde yer alan bilgi teknolojilerinin öneminin artması, operasyonları yürüten işletmeye ait gerçekleştirilecek olan denetim faaliyetlerinde, denetim amaçlarının etkin ve verimli bir şekilde sağlanabilmesi için bilgi sistemleri denetim faaliyetlerinden de yararlanmanın kaçınılmaz olduğunu ortaya koymaktadır.

Bankacılık sektöründe faaliyet gösterilen iş süreçleri kapsamında öncelikli olarak süreç kapsamının tam ve doğru bir şekilde incelenmesi buna bağlı olarak süreç içerisinde yer alan risklerin tespit edilip, söz konusu risklerin öneminin ve etkisinin COBIT **uygulama kontrolleri ile genel kontrollerin** derecesi belirlenmelidir.

Banka bünyesinde belirlenen risklerin kontrol edilmesini sağlayacak kontrol mekanizmalarının oluşturulması aşamasında, kontrollerin manuel olması durumunda COSO kontrol hedeflerinin, kontrollerin otomatik olması durumunda ise COBIT kontrol hedeflerinin dikkate alınması sağlanmalıdır.

Süreç içerisinde oluşturulacak kontroller çerçevesinde, kontrol hedeflerinin karma şekilde kullanılması, riskin yönetilmesi aşamasında önemli bir etki yaratacaktır.

Süreç içerisinde belirlenen risk ve kontrollerin periyodik olarak risk kontrol kataloğu kapsamında gözden geçirilmesi gereklidir.

Gerçekleştirilen uygulama sonucunda bankacılık sektöründe bireysel krediler sürecine sahip olan bir banka için, ideal ve her banka bünyesinde uygulanabilir olan, otomatik-manuel kontrollerin yer aldığı risk kontrol matrisi oluşturulmuştur.

Araştırmanın uygulanması kapsamında yapılan değerlendirmeler ile aşağıdaki sonuç ve önerilere varılmıştır:

- Bankacılık faaliyetlerine konu olan bütün iş süreçlerinin analiz edilmesi ve söz konusu analiz kapsamında risklerin uygulanan kontrollerden bağımsız olarak değerlendirilmesi ve yapılan değerlendirme sonucunda tespit edilen riskleri yönetecek ve kontrol edecek olan kontrol faaliyetlerinin COSO ve COBIT kontrol hedefleri dikkate alınarak kurgulanması ve söz konusu kontrol faaliyetlerinin periyodik olarak kontrollerinin gerçekleştirilmesi sağlanmalıdır.
- Bankalar bünyesinde yürütülen faaliyetlere ait risklerin belirlenmesi ve söz konusu risklere ait COSO ve COBIT kontrol hedefleri kapsamında kontrol mekanizmaların oluşturulması;
  - Gerçekleştirilen faaliyetlerin daha hızlı, verimli ve etkili olarak yapılmasını,
  - Faaliyetler kapsamında oluşturulan bilgilerin bütünlüğünün ve güvenirliliğinin artmasını,
  - Süreç kapsamında gerçekleştirilecek olan kontrollerin daha kısa sürede incelenmesini ve uygulanmasını sağlayacaktır.
- COSO modeli içerisinde yer alan uygulama kontrolleri alanı bankaların teknoloji yoğun iş süreçlerini ve iç kontrol ortamını değerlendirmek için gerekli noktaları kapatarak, günümüz gereği olan entegre kontrol yapısının oluşmasını sağlamaktadır. Bankalar bünyesinde yürütülen faaliyetlere ait uygulama kontrolleri alanının tanımlanmış olması, yürütülen faaliyetlere ait risklerin tamamen ortadan kaldırılması anlamına gelmeyecektir. Bu kapsamda süreç ve faaliyetler kapsamında genel kontrol alanlarının da oluşturulması sağlanmalıdır. Bankalar tarafından kullanılan uygulamalar üzerinde tasarlanan kontrollerin etkin

bir bilgi teknolojileri genel kontrol ortamı üzerinde çalışması sağlanmalıdır. Güvenli olmayan bir bilgi teknolojileri genel kontrol ortamı üzerinde tesis edilen uygulama kontrollerinin (manuel ve/veya otomatik) etkin olarak çalışması söz konusu kontrollerin güvenilir olduğu anlamına gelmeyecektir. Bu nedenle, süreç kapsamında tasarlanan uygulama kontrollerinin güvenilirliğini artıracak olan genel kontrol ortamlarının oluşturulması ve periyodik olarak gözden geçirilmesi sağlanmalıdır.

- Bankacılık faaliyetleri ile ilgili olarak gerek iç gerekse bağımsız denetim kapsamında, finansal denetim amaçları ile bankacılık sektöründeki bilgi sistemleri denetim faaliyetleri kapsamındaki uygulama denetimi sonuçlarının bir arada değerlendirmesi ve entegre denetim faaliyetleri ile desteklenmesi sağlanmalıdır.

KAYNAKÇA

Kitaplar:

AKÇAY M. Barış ve BOLGÜN K. Evren. **Risk Yönetimi: Gelişmekte Olan Türk Finans Piyasasında Entegre Risk Ölçüm ve Yönetim Uygulamaları**, 2. Baskı, Scala Yayıncılık, İstanbul, 2005.

ANAND, Sanjay. **Sarbanes- Oxley Guide for Finance and Information Technology Professionals**, John Wiley&Sons, Inc., Vol:2, 2006.

BESSIS, Joel. **Risk Management in Banking**, 2. Baskı, İngiltere: John Wiley&Sons Ltd., 2002.

BOLGÜN Evren ve AKÇAY Barış. **"Sermaye Piyasası ve Reel Sektör Uygulamaları"**, Scala Yayıncılık, 3. Baskı, İstanbul, 2009.

ÇITAK, Serdar. "Geleneksel Risk Yönetiminden Programlanmış Menkul Kıymet İşlemlerine, Ekonomi Dizisi:7", **Dünya Yayınları**, İstanbul, Ekim 1999.

KESKİN, Duygu Anıl. **İç Kontrol Sistemi Kontrol Öz Değerlendirme**, Beta Yayınları, İstanbul, 2006.

MCLEOD, Reymond. **Management Information Systems**, 4.b., New York: Macmillan, 1990.

ŞAKAR, Hakan. **Bankalarda Kredilendirme Teknikleri,** 1. Basım, Mida Yayınları, İstanbul, 2003.

TANSEL TUĞCU Can ve ERDEM Ekrem. **Bankalarda Kredi Yönetimi**, Anadolu Üniversitesi, 1.Baskı, Eskişehir, Haziran 2012.

UYEMURA, D.G. **Financial Risk Management in Banking**, Bankers Publishing Company, Chicago, 1993.

WESTON J.F. ve BRIGHAM F.E. **Managerial Finance**, Dryden Press:5th Ed., London, 1975.

YILANCI, Münevver. **İç Denetim: Türkiye'nin 500 Büyük Sanayi İşletmesi Üzerine Bir Araştırma**, Nobel Yayın Dağıtım, 2. Baskı, Eskişehir, 2006.

YÜKSEL A.Sait, YÜKSEL Aslı ve YÜKSEL Ülkü. **Bankacılık Hukuku ve İşletmesi**, Beta Yayınları, 10.Bası, İstanbul 2004.

Dergiler:

AKSOY, Tamer. "Ulusal ve Uluslararası Düzenlemeler Bağlamında İç Kontrol ve İç Kontrol Gerekliliği: Analitik Bir İnceleme", **Mali Çözüm Dergisi**, Sayı:72, 2005.

AKYEL, Recai. "Türkiye'de İç Kontrol Kavramı, Unsurları ve Etkinliğinin Değerlendirilmesi", **Celal Bayar Üniversitesi İİBF Yönetim ve Ekonomi Dergisi**, Cilt:17, Sayı:1, 2010.

ALP, İnönü Akgün. "Bankalarda Karapara Aklama Risk Yönetimi", **Active Bankacılık ve Finans Dergisi**, Sayı:145, Ocak-Şubat 2005.

ANAMERİÇ, Hakan. "Yönetim Bilgi Sistemlerinin Yönetim Fonksiyonları Üzerine Etkisi", **Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi**, Sayı:2, 2005.

ARAS, Güler. "Basel II Bankacılık Düzenlemeleri ve İç Denetim", **TİDE İç Denetim Dergisi**, Sayı:17, 2007.

ARAŞTIRMA, Active. "Bankalarda Performans ve Risk Yönetimi: Analitik bir Çerçeve", **Active Bankacılık ve Finans Dergisi**, Sayı:15, Ekim-Kasım 2000.

ATMACA, Metin. "Muhasebe Skandallarının Önlenmesinde İç Kontrol Sisteminin Etkinleştirilmesi", **Afyon Kocatepe Üniversitesi İİBF Dergisi**, Cilt:14, Sayı:1, 2012.

AYANOĞLU Yıldız ve ERTÜRK Burak. "Modern Kredi Riski Yönetiminde Derecelendirmenin Yeri ve İMKB'ye Kayıtlı Şirketler Üzerinde Bir Uygulama**", Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Sayı:9, Şubat 2007.

BAKKAL Hakan ve KASIMOĞLU Alper. "İç Kontrol Sistemine Karşılaştırmalı bir bakış "COSO ve COCO Modeli", **Mevzuat Dergisi**, Sayı:178, Ekim 2012.

BOYACIOĞLU, Melek Acar. "Operasyonel Risk Yönetimi", **Bankacılar Dergisi**, Sayı:43, 2002.

BOZKURT Nejat. İBİŞ, CEMAL. ve AKDEMİR, Çağla. "6102 Sayılı Türk Ticaret Kanunu Kapsamında Bağımsız Denetim ve Hile Riski", **Dış Denetim Dergisi**, Ekim-Kasım-Aralık 2011.

BOZKUŞ, Kahyaoğlu Sezer. "Kurumsal Risk Yönetimi", **KPMG Gündem Dergisi**, Sayı: 9, Ocak-Mart 2012.

CANDOĞAN Mehmet Ali ve ALTAN Mikail. "Basel Kriterleri Çerçevesinde Operasyonel Risk Ölçüm Yöntemlerinin Karşılaştırılması: Örnek Bir Uygulama", **Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Sayı:31, 2014.

CEYLAN Hüseyin ve S. BAŞHELVACI Volkan. "Risk Değerlendirme Tablosu Yöntemi ile Risk Analiz: Bir Uygulama", **International Journal of Engineering Research and Development**, Cilt 3, Sayı 2, Haziran 2011.

CEYLAN İsmail Fatih ve APAN Mehmet. "Coso İç Kontrol Modeli"nin Yapısal Eşitlik Modeli ile İncelenmesi: Bir Hastane Uygulaması", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt: 6, Sayı:10, Haziran 2014.

ÇAĞDAŞ Berk ve GÜRSOY Cudi Tuncer. "Şirketlerde Finansal Risk Yönetimi Amaçlı Bir Modelin Geliştirilmesi Yöntem ve Aşamaları", **İTÜ Dergisi**, Cilt:2, Sayı:3, Haziran 2003.

DEMİREL H. Gökçe ve YARDIMCIOĞLU Mahmut. "Risk Yönetiminde Kriz Sonrası Yeni Finansal Mimariye Yönelik Bir Adım: Basel III", **Mali Çözüm Dergisi**, Sayı:125, Kasım-Aralık 2010.

DEMİRHAN, Dilek. "İşletmelerde Stratejik Bilgi Sistemleri Yönetimi ve Rekabet Üstünlüğü Elde Edilmesindeki Rolü", **Ege Akademik Bakış Dergisi**, Cilt:2, Sayı:2, Temmuz 2002.

DİNÇ, Berna. "Mali Denetimde Önemlilik Kavramı", **Sayıştay Dergisi**, Sayı:50-51, Temmuz-Aralık 2003.

DUMANOĞLU Sezai ve ERGÜL Nuray. " Basel 2'nin KOBİ'ler Üzerindeki Muhtemel Etkileri", **Muhasebe ve Finansman Öğretim Üyeleri Bilim ve Araştırma Derneği Muhasebe ve Finansman Dergisi**, Sayı:43, Temmuz 2009.

ELİTAŞ, Cemal. "Kontrol Önlem ve Yordamlarının İç Denetçi Açısından Rolü ve Önemi", **İç Denetim Dergisi**, Sayı:8, 2004.

ENE, Selda. " Proje Yönetiminde Yer Alabilecek Risk Kaynaklarının Tespiti ve Risk Yönetim Planının Geliştirilmesi", **İstanbul Sosyal Bilimler Dergisi**, Sayı:5, 2013.

ERMİSKET, Evren Güncel. "Kamu Kurumlarında Risk Yönetimi-Bir Uygulama Önerisi", **Kamu İç Denetçileri Derneği Denetişim Dergisi,** Sayı:7, 2011.

EROL, Mikail. "Basel I ve Basel II Uzlaşısının Bankalar Tarafından İşletmelere Verilen Kredilerde Risk Yönetimi Aracı Olarak Kullanılması", **Muhasebe ve Finansman Öğretim Üyeleri Bilim ve Araştırma Derneği Muhasebe ve Finansman Dergisi**, Sayı:36, Ekim 2007.

GÖÇEN, Ceren Ayça. "Kurumsal Yönetim, İç Kontrol ve Bağımsız Denetim: Parmalat Vakası", **Mali Çözüm Dergisi**, Sayı: 97, 2010.

GÜNEY, Cengiz. "Bilgisayarlı Muhasebe Sistemlerinde Denetim Riskleri ve Bilgisayar Destekli Denetim Teknikleri", **Akademik Sosyal Araştırmalar Dergisi**, Sayı:28, Temmuz 2016.

GÜREL Eymen, BULGURCU GÜREL, Esra Burcu ve DEMİR Neslihan. "Basel III Kriterleri", **Bankacılık ve Sigortacılık Araştırmaları Dergisi**, Cilt:1, Sayı:3-4, Ocak 2012.

GÜVEN, Aytekin. “Yatırımlar, Belirsizlik ve Piyasa Yapısı: Kavramsal Bir İnceleme”, **Afyon Kocatepe Üniversitesi İBBF Dergisi**, Cilt:15, Sayı:1, 2013.

HATUNOĞLU Zeynep, KOCA Nurettin ve KILLI Mustafa. “İç Kontrolün Muhasebe Sistemindeki Hata ve Hilelerin Önlenmesindeki Rolü Üzerine Bir Alan Çalışması”, **Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt:9, Sayı:20, 2012.

HENDERSON J.C. and VENKATRAMAN N. “Strategic alignment: Leveraging information technology for transforming organizations”, **IBM Systems Journal**, Vol: 32, no:1, 1993.

HESCHI, Jimmy. “ Mapping ITILv3 to COBIT”, **COBIT Focus**, Ocak 2008.

HUGHES, Greg. “IT Risk Management Report”, **Symantec Corporation**, Volume 1, February 2007.

IMMANENI Aravind, MASTRO Chris ve HAUBENSTOCK Michael. “A Structured Approach to Building Predictive Key Risk Indicators”, **Operational Risk: A Special Edition of The RMA Journal**, May 2004.

IŞIN, Feride Bahar. “Teknoloji Araçlarının Bankacılık Sektöründe Uygulanabilirliği ve Türkiye’deki Bu Doğrultudaki Bankacılık Uygulamalarının Değerlendirilmesi”, **İktisadi ve İdari Bilimler Dergisi**, Cilt:20, Sayı:2, Eylül 2006.

İBİŞ Cemal ve ÇATIKKAŞ Özgür. “İşletmelerde İç Kontrol Sistemi’ne Genel Bakış”, **Sayıştay Dergisi**, Sayı:85, Nisan-Haziran 2012.

KIZILBOĞA Ruveyda ve ÖZŞAHİN Filiz. ”Etkin Bir İç Kontrol Sisteminin İç Denetim Faaliyetine ve İç Denetçilere Katkısı”, **Niğde Üniversitesi İİBF Dergisi**, Cilt:6, Sayı:2, 2013.

KOÇ, Selahattin. “Bankaların Karşılaştıkları Riskleri Yönetmedeki Etkinliği: Türkiye Ölçeği”, **Maliye Dergisi**, Sayı:165, Temmuz-Aralık 2013.

KOÇYİĞİT ÇİL Seyhan ve DEMİR Aysel. "Türk Bankacılık Sektöründe Kredi Riski ve Yönetimine İlişkin Bir Uygulama: Türkiye Garanti Bankası Örneği", **İşletme Araştırmaları Dergisi**, Sayı:309, Temmuz 2012.

LAWTON, Robert. "Transitioning IT From a Compliance to a Value-Driven Enterprise Using CobiT", **Information Systems Control Journal**, volume:6, 2007.

MAES Rik, RİJSENBRİJ Daan, TRUİJENS Onno ve GOEDVOLK Hans. "Redefining business-IT alignment through a unified framework", **Primavera Working Paper Series- Amsterdam University**, June 2000.

MANDACI, Pınar Evrim. "Türk Bankacılık Sektörünün Taşıdığı Riskler ve Finansal Krizi Aşmada Kullanılan Risk Ölçüm Teknikleri", **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Cilt 5, Sayı 1, 2003.

OKTAY Sadiye ve TEMEL Halim. **"**Basel II Kriterleri Ekseninde Ticari Bankalarda Kredi Riski Yönetiminin Karşılaştırılmasına Yönelik Bir Saha Çalışması", **Zonguldak Karaelmas Üniversitesi Sosyal Bilimler Dergisi**, Cilt:3, Sayı:6, 2007.

ÖMÜRBEK Vesile ve ALTAY Sevil Özge. "Turizm İşletmelerinde İç Kontrol Sisteminin Etkinliğinin İncelenmesi ve Manavgat Bölgesindeki Beş Yıldızlı Otellerde Bir Araştırma", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Cilt:16, Sayı:1, 2011.

ÖZBİLGİN, İzzet Gökhan. "Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar", **Sayıştay Dergisi**, Sayı:49, Nisan-Haziran 2003.

SAYIM Ferhat ve ER Selami. "Risk Kavramı ve Bankacılıkta Risk"**, TMSF Çatı Dergisi**, Sayı:22, Temmuz-Ağustos-Eylül 2009.

SELİMLER, Hüseyin. "Sorunlu Kredilerin Analizi, Banka Finansal Tablo Oranlarına Etkisinin Değerlendirilmesi", **Finansal Araştırmalar ve Çalışmalar Dergisi**, Cilt:7, Sayı:12, Ocak 2015.

SELVİ, Özgür. “Bilgi Toplmu, Bilgi Yönetimi ve Halkla İlişkiler”, **Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi**, Sayı:3, Mart:2012.

ŞAHİN, İlhan. “Küresel Finansal Kriz Esnasında Geliştirilen Bankacılık Düzenlemelerinden Basel III kriterlerinin Kapsamı ve Uygulama Süreci”, **Muhasebe ve Finansman Dergisi**, Temmuz 2013.

ŞENDOĞDU A. Aslan. “Basel II Kriterlerinin Dünü Bugünü ve Gelecek İçin Bir Üst Sürümüne Olan İhtiyacın Kaçınılmazlığı”, **Bankacılık ve Sigortacılık Araştırmaları Dergisi**, Cilt:1, Sayı:2, Haziran 2010.

TÜREDİ Hasan ve ALICI Ümmügülsüm. “Mali Raporlama Hilelerinin Tespit ve Önlenmesinde İç Kontrol Yapısının Önemi”, **Finansal Araştırmalar ve Çalışmalar Dergisi**, Cilt:6, Sayı:11, Temmuz 2014.

TÜREDİ Hasan ve KARAKAYA Gencay. “COSO İç Kontrol Modeli ve Kontrol Ortamı”, **Finans Politik ve Ekonomik Yorumlar Dergisi**, Cilt:52, Sayı:602, 2015.

TÜREDİ Hasan ve KOBAN Ahmet Oğuz. “COSO İç Kontrol Modelinde Risk Değerlendirme Faaliyetleri”, **Marmara Üniversitesi Öneri Dergisi**, Cilt:12, Sayı:46, Temmuz 2016.

UMUT UYSAL, Ertuğrul. “Operasyonel Risk Yönetiminde Senaryo Analizi”, **Bankacılar Dergisi**, Sayı:69, 2009.

UYAR Süleyman ve AYGÖREN Hakan. “Basel II İlkelerinin KOBİ’lere Olası Etkileri: Finansman Maliyeti, Finansal Raporlama ve Muhasebe Açısından Değerlendirme”, **Mali Çözüm Dergisi**, Sayı: 77, Ağustos-Eylül-Ekim 2006.

UZAY, Şaban. “İşletmelerde İç Kontrol Sistemini İncelemenin Bağımsız Dış denetim Karar Sürecindeki Yeri ve Türkiye’deki Denetim Firmalarına Yönelik Bir Araştırma”, **Sermaye Piyasası Kurulu**, Yayın No:132, Ankara, 1999.

ÜVEY, Mehmet Cüneyt. “Orkestra Şefiniz: COBIT”, **CIO Club**, Mayıs 2009.

WESTERMAN George ve HUNTER Richard. "IT Risk Turning Business Threats into Competitive Advantage", **Harvard Business School Press**, June 2007.

YALÇINKAYA, Timuçin. "Risk ve Belirsizlik Algılamasının İktisadi Davranışlara Yansımaları", **Muğla Üniversitesi İİBF Tartışma Tebliğleri**, No:2004/05, 2004.

YARDIMCIOĞLU Mahmut ve BAY Murat. "Türkiye'de Basel II'nin Kobilere Uygulanma Sorunları ve 2009 Yılı Bankacılık Sektörü Analizi", **Mali Çözüm Dergisi**, Sayı:101, Eylül-Ekim 2010.

YARIZ, Ahmet. "Bankacılıkta Risk Yönetimi: Risk Matrisi Uygulaması", **Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü E-Dergisi**, Sayı 1, Temmuz 2011.

YAY Turan, GÜRKAN YAY Gülsün ve YILMAZ Ensar. "Finansal Krizler, Finansal Regülasyon ve Türkiye", **İstanbul Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Sayı:30, Mart 2004.

YİĞİT Sema ve YİĞİT Alperen M. "Stratejik Yönetimde Dış Çevre Analizi: Kobi'ler ve Büyük İşletmeler Arasında Bir Karşılaştırma", **Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, Sayı:38, Haziran-Aralık 2011.

YURTSEVER, Gürdoğan. "Bankacılığımızda İç Kontrol", **TBB Yayınları**, No:256, 2008.

YÜKSEL MERMOD Aslı ve CERAN Mustafa. "Basel III Doğrultusunda Bankacılık Riskleri ve Sermaye Yeterliliği; Türk Bankacılık Sektörü Üzerine Karşılaştırmalı Bir Analiz", **Finansal Araştırmalar ve Çalışmalar Dergisi**, Cilt:2, Sayı:4, 2011.

Tezler:

ALİKADIOĞULLARI, Arzu. "Türkiye'de Mali Reform Kapsamında İç Kontrol Sistemi Uygulaması Maliye Bakanlığı Örneği", **Yüksek Lisans Tezi**, Isparta: Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, 2011.

ALOĞLU, Ziya Tunç. "Bankacılık Sektörünün Karşılaştığı Riskler ve Bankacılık Krizleri Üzerindeki Etkileri", **Uzmanlık Yeterlilik Tezi**, TCMB Bankacılık ve Finansal Kuruluşlar Genel Müdürlüğü, Mart 2005.

ARSLAN, Dilek. "Bankacılık Sektöründe Kredi Kullanıcılarının Değerlendirilmesi", **Yüksek Lisans Tezi**, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2014.

BALKAŞ, Kaan. "Kredi Kavramı ve Sektör Kredilerine Göre Türkiye'deki Belli Başlı Sektörlerin Analizi", **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2004.

BAŞARIR, Mustafa. "Bankalarda Teknoloji Riski ve Yönetimi", **Yüksek Lisans Tezi**, İstanbul: Marmara Üniversitesi, Bankacılık ve Sigortacılık Enstitüsü, 2006.

BİLGE, Gökhan. "Bankalar Açısından Risk Yönetiminin Önemi ve Basel II Sürecinin Risk Yönetimi Üzerindeki Etkileri", **Yüksek Lisans Tezi**, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta, 2011.

CENGİZ, Efsane. "Basel I-II-II Sermaye Uzlaşısı", **Yüksek Lisans Tezi**, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2013.

ÇATIKKAŞ, Özgür. "Bankalarda İç Kontrol Sistemi ve İç Denetim Fonksiyonunun Etkililiği", **Doktora Tezi**, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü Bankacılık Anabilim Dalı, İstanbul, 2005.

ÇİFTÇİ, İlhan. "Basel II Çerçevesinde Operasyonel Risk İçin Sermaye Ayarlaması", **Yüksek Lisans Tezi**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2007.

DOĞANTİMUR, Fulya. “ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği”, Maliye Bakanlığı Strateji Geliştirme Başkanlığı **Mesleki Yeterlilik Tezi**, 2009.

EMRE ULTAV, Ekrem. “Bilgi Sistemlerinin İşletmeler için Stratejik Önemi ve Başarısının Ölçülmesi”, **Yüksek Lisans Tezi**, İstanbul, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2010.

ERZİ, Handan. “Sarbanes-Oxley Yasasının Yolsuzluk Vakalarının Ortaya Çıkarılmasındaki Rolü: Yasa Öncesi ve Sonrasında Yaşanan Şirket Yolsuzluk Vakaları Üzerine Mukayeseli Bir İnceleme”, **Yüksek Lisans Tezi**, Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü, Hatay, 2010.

GÜNEŞ, Şükran. “İşletmelerde Hile Riskinin Önlenmesi ve Hastane İşletmelerinde Uygulama”, **Yüksek Lisans Tezi**, İşletme Anabilim Dalı, İstanbul, 2014.

KAPAĞAN, Gönül. “Bağlı Tüketici Kredileri”, **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2004.

KARA, Ömer. “Bankalarda Operasyonel Risk”, **Yüksek Lisans Tezi**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, Haziran 2009.

KIRMIZI, Nihat. “İşletmelerde İç Kontrol Sistemini İncelemenin Bağımsız Denetim Karar Sürecindeki Yeri”, **Yüksek Lisans Tezi**, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2007.

KORKUT, Beliz. “Merkez Bankalarında İç Kontrol ve Risk Ölçümü Uygulamalarının TCMB Kambiyo Muhasebesi İşlemleri Açısından Değerlendirilmesi”, **Uzmanlık Tezi**, TCMB Muhasebe Genel Müdürlüğü, Şubat 2004.

ÖKER, Ayşegül. “Ticari Bankalarda Kredi ve Kredi Riski Yönetimi-Bir Uygulama”, **Doktora Tezi**, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2007.

ÖZÇELİK, Osman. “Bankacılıkta Risk Analizi, Yönetimi ve Riskten Korunma”, **Yüksek Lisans Tezi,** Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Edirne, Ocak 2006.

ÖZGÜN, Tolga. “Bilişim Teknolojileri ile İşletme Stratejileri Arasındaki Uyumun Faktör Analizi Yöntemi ile Ölçülebilirliği”, **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2015.

ÖZGÜR ÖZDEN, Kürşat. “Ticari Bankalarda Kredilendirme Süreci ve Kredi Riski Yönetimi”, **Yüksek Lisans Tezi**, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir, 2010.

SOLAŞ, Çiğdem. “Bankalarda İç Denetim Tekniği ve Türk Uygulaması”, **(Yayınlanmamış Doçentlik Tezi)**, Marmara Üniversitesi, İstanbul, 1975.

SOYER, Semih. “Uluslararası Denetim Standartları”, **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2005.

SÜMER, Ebru. “Türkiye’de Kamu İç Kontrol Sistemi Kapsamında Hesap Verme Mekanizmaları”, **Mesleki Yeterlilik Tezi**, T.C Maliye Bakanlığı Strateji Geliştirme Başkanlığı, 2010.

ŞİMŞEK, Kemal Çağatay. “Bankacılıkta Risk ve Risk Ölçüm Yöntemleri”, **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2007.

TOKEL, Ömer Emre. “Kredi Risk Modelleri Kullanılarak Kredi Taleplerinin Değerlendirilmesi”, **Yüksek Lisans Tezi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2004.

YILDIRIM, Ezgi. “Bankalarda Ticari Kredilendirme Süreci; Karşılaşılan Sorunlar ve Çözüm Yolları İle İlgili Ampirik Bir Çalışma”, **Yüksek Lisans Tezi**, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2007.

YILMAZ, Songül. “Ticari Bankalarda Kredi Portföyü ve Kredi Riski Yönetimi-Bankacılık Sektöründe Bir Uygulama”, **Yüksek Lisans Tezi**, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2010.

İnternet Adresleri:

ALAGÖZ, Ali. İşletmelerde İç Kontrol Sisteminin Önemi ve Denetim Komiteleri ile İç Denetim Birimi İlişkisinin Hata ve Hilelerin Önlenmesindeki Rolü, http://www.alialagoz.com.tr/doc-dr-alialagoz-makaleleri/isletmelerde_ic_kontrol.pdf, (27.09.2011).

ARCAGÖK, M. Sait. Yeni Mali Yönetim ve Kontrol Sisteminde İç Kontrol, **Maliye Bakanlığı Bütçe ve Mali Kontrol Genel Müdürlüğü**, Kızılcahamam, 09.09.2006, http://kontrol.bumko.gov.tr/Eklenti/4033,kizilcihamamsunumupdf.pdf?0, (07.08.2013).

ARI, Mustafa. "Finansal Raporlama Skandalları ve Mali Tabloların Güvenirliliği", http://birimler.dpu.edu.tr/app/views/panel/ckfinder/userfiles/17/files/DERG_/23/409-420.pdf, (07.07.2015).

ARSLAN, Nurtaç. "İç Kontrol Sistemi Sunumu", T.C Strateji Geliştirme Başkanlığı http://www.strateji.gov.tr/ortak_icerik/strateji/ickontrolcalismalari/sunumlar/ickontrolicislerisunumNurtacarslan.ppt, (16.04.2010).

ARTİNYAN, Eliza Natasa. "Cobit Çerçevesi", Deloitte Yayınları, 2007, http://www.denetimnet.net/UserFiles/Documents/Makaleler/BT%20Denetim/CobiT%20%C3%87er%C3%A7evesi.pdf, (24.06.2012).

BAĞCI, Barış. "Bilgi Teknolojileri Risk Yönetimine Genel Bakış", 2007, http://www.denetimnet.net/UserFiles/Documents/DeloitteMakaleleri/Bilgi%20Teknolojileri%20Risk%20Y%C3%B6netimine%20Genel%20Bak%C4%B1%C5%9F.pdf, (08.07.2013).

BAZIBAŞ, Murat. Operasyonel Risk ve Veri Tabanı Modellemesi, **BDDK Çalışma Raporları**, Mart 2006, http://www.bddk.org.tr/WebSitesi/turkce/Basel/12922006-2.pdf, (11.12.2014).

BOZKUŞ, Kahyaoğlu Sezer. Kurumsal Risk Yönetimi Standartları-Yeni Türk Ticaret Kanunu Çerçevesinde Türkiye Uygulaması, 2012,

http://www.gtturkey.com/ud_objs/pdf/etknlk/musiad_risk_yonetimi_sunumu.pdf, (09/05/2014).

COMMITTEE, Basel. Operational Risk, 2001, http://www.bis.org/publ/bcbsca07.pdf, (15.10.2005).

COMMITTEE, Basel. Principles for the Management of Credit Risk, 1999, http://www.bis.org/publ/bcbs75.pdf, (05.06.2012).

COSO. Fraudulent Financial Reporting: 1987-1997 An Analysis of U.S Public Companies, http://www.coso.org/documents/FFR_1987_1997.PDF, March 1999, (09.07.2014).

COSO. Internal Control Over Financial Reporting Guidance for Smaller Public Companies, http://www.coso.org/documents/sb_executive_summary.pdf, June 2006, (09.07.2014).

COSO. Internal Control-Integrated Framework-Guidance on Monitoring Internal Control Systems, http://www.coso.org/documents/volumeii-guidance.pdf, June 2008, (09.07.2014).

COSO. Report of the National Commission on Fraudulent Financial Reporting, http://www.coso.org/Publications/NCFFR.pdf, October 1987, (12.06.2014).

ÇUBUKÇU, Faruk. "İşletme Yönetimi ve Bilgi Sistemleri", Yüksek Lisans Tezi, http://www.farukcubukcu.com/images/docs/yonetimbilgisistemleri.htm, (19.06.2007).

ERDOĞAN, Nurten. "Muhasebe Denetiminde Niteliksel Önemliliğin Gerekliliği", http://www.journal.mufad.org.tr/attachments/article/435/13.pdf, (25.05.2013).

GEGİN, Eren. "İç Denetimde Bilgi Sistemleri Denetiminin Yeri", BTYD 2010, http://www.btyd.org.tr/kategori/25979-program, (28.04.2011).

GÜLTEKİN, Tumin. "Finansal Denetimde İç Kontroller", BTYD 2010, http://www.btyd.org.tr/kategori/25979-program, (28.04.2011).

GÜVERCİNCİ, Oya. "Bankalarda Risk Yönetimi", 15.03.2011, http://www.riskonomi.com/wp/?p=392, (15.03.2011).

INTOSAI, http://www.intosai.org/, (10.01.2014).

İç Denetim Enstitüsü, "Terimler Sözlüğü: Kontrol (Control)", http://www.tide.org.tr/page.aspx?nm=terimler_sozlugu, (08.09.2010).

KPMG Türkiye Finansal Danışmanlık Hizmetleri. "Türkiye'de ve Dünyada Bankacılık Sektörü Risk Yönetimi Uygulamaları ve Düzenlemeleri", 17 Aralık 2009, http://www.tbb.org.tr/Dosyalar/Konferans_Sunumlari/RiskYonetimi17.12.2009.zip, (13.12.2015).

OpRisk Dergisi. "Barings Bank'ın İflas Öyküsü", http://www.opriskdergisi.com/oprisk-ornek-22-barings_bankin_iflas_oykusu.html, (24.03.2014).

PRIANDOYO, Anjar. "Comparison between COBIT, ITIL and ISO 27001", 2012, http://www.securityprocedure.com/comparison-between-cobit-itil-and-iso-27001, (02.06.2015).

Pricewaterhousecoopers. Kurumsal Risk Yönetimi Temel Kavramlar ve Uygulamalar, 2007, https://www.vergiportali.com/doc/fuar2007/kurumsalriskyonetimi.pdf, (12.03.2010).

Sarbanes-Oxley Act. Public Law 107-204, https://www.sec.gov/about/laws/soa2002.pdf, July 30, 2002, (09.06.2015).

ŞEN, Yalçın Ümit. "Bilgi Teknolojileri Denetiminde Kontrol Tipleri", BTYD 2010, http://www.btyd.org.tr/kategori/25979-program, (28.04.2011).

T.C Strateji Geliştirme Başkanlığı, "COSO Kurumsal Risk Yönetim Bütünleşik Çerçevesi Ana Metni-Çeviri", http://www.sgb.gov.tr/IcKontrol/KontrolStandartlarYeni/Dokümanlar/Çeviriler/İç Kontrol Bütünleşik Çerçeve-COSO.pdf, (14.10.2011).

UZUNAY, Vildan. “COBIT (Control Objectives for Information and Related Technology)” 2007, http://kontrol.bumko.gov.tr/Eklenti/4045,cobitpdf.pdf?0, (18.01.2014).

VARL,I Ahmet Türkay. ”Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi- Mevzuat Çerçevesinde BDDK Perspektifi”, 09.11.2007, www.bddk.org.tr/WebSitesi/turkce/Raporlar/Sunumlar/4020TIDE_Sunum.pdf, (12.03.2010).

YURTSEVER, Gürdoğan. Bankacılığımızda İç Kontrol, **TBB Yayınları**, No:256, İstanbul, Nisan 2008, http://www.tbb.org.tr/Dosyalar/Yayinlar/Dokumanlar/2ickontrol.pdf, (24.03.2011).

Tebliğ ve Yönetmelikler:

BDDK, “5411 Sayılı Bankacılık Kanunu”, Sayı: 25983, Tarih:1 Kasım 2005.

BDDK, “Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik”, Madde 25, Sayı 27461, Tarih: 13 Ocak 2010.

BDDK, “Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik”, Madde 18, Sayı 26170, Tarih: 16 Mayıs 2006.

BDDK, “Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik” Madde 1, Sayı 26170; Tarih: 16 Mayıs 2006.

BDDK, “Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ” Madde 5, Sayı: 26643, Tarih:14 Eylül 2007.

BDDK, “Bankalarda Bilgi Sistemleri Yönetmeliğinde Esas Alınacak İlkelere İlişkin Tebliğ”, Madde:22, Sayı:26643; Tarih:16 Eylül 2007.

BDDK, “Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmelik”, 08.02.2001.

BDDK, “Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmeliğin Uygulanmasına ilişkin 1. Sayılı Tebliğ” , 08.02.2001.

BDDK, “Bankaların Kredi Yönetimine İlişkin Rehber”, Sayı: 6462, Tarih:17 Eylül 2015.

Araştırma ve Raporlar:

ARSLAN, Işılda. **“Kurumsal Risk Yönetimi”**, Maliye Bakanlığı Strateji Geliştirme Başkanlığı 2008.

AYKUT Nursu. “ Türk Bankacılık Sektörünün İç Kontrol Sistemi ve Risk Yönetimi Açısından Değerlendirilmesi ve Bu Bağlamda Basel II Kriterlerinin Sektöre Etkileri”, **Dönem Projesi**, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2011.

Basel Committee on Banking Supervision, “ The Internal Audit Function in Banks”, June 2012.

BDDK. “ Bankacılık Değerlendirme Raporu”, Ekim 2004.

DURAN Erdal. “Kamu İdarelerinde Kurumsal Risk Yönetimi Uygulamaları”, **Mali Hizmetler Uzmanlığı Araştırma Raporu**, Ankara, 2013.

Maliye Bakanlığı Strateji Geliştirme Daire Başkanlığı. “Kurumsal Risk Yönetimi Dokümanı”, Mart 2008.

MAZIBAŞ Murat. **“Operasyonel Riske Basel Yaklaşımı: Risk Verilerine İlişkin Bir Değerlendirme”**, BDDK Araştırma Raporları, Temmuz 2005.

TBD Kamu-BİB Kamu Bilişim Platformu 8, “Bilişim Teknolojilerinde Risk Yönetimi”, **Çalışma Grubu**, 27 Mart 2006.

TUNÇ İlker. “Kurumsal Risk Yönetim Sisteminin Stratejik Planlamanın Başarısı Üzerindeki Etkisi”, **Mali Hizmetler Uzmanlığı Araştırma Raporu**, Yalova, Mart 2014.

TÜSİAD. “Kurumsal Risk Yönetimi”, **Kurumsal Risk Yönetimi Grubu Çalışması**, Aralık 2006.

Diğer Kaynaklar:

AIRMIC (The Association of Insurance and Risk Managers). "**A Risk Management Standard"**, 2002.

BELLINO Christine, WELLS Jefferson, HUNT Steve ve HORWARTH LLP Crowe, **Global Technology Audit Guide (GTAG) 8: Auditing Application Controls**, The Institute of Internal Auditors, January 2009.

COSO Enterprise Risk Managament Integrated Framework - Executive Summary, "Internal Environment – The internal environment encompasses the tone of an organization", September 2004.

ISACA, "COBIT 4.1 Framework Control Objectives Management Guidelines Maturity" Models, 2007.

ISACA, "Control Objectives for Information and related Technology 4.0 (USA)", 2005.

IT GOVERNANCE INSTITUTE, "IT Control Objectives for Sarbanes-Oxley: The Role of IT In The Design and Implementation of Internal Control Over Financial Reporting", 2nd Edition, USA, September 2006.

İMKB, "Sermaye Piyasası ve Borsa Temel Bilgiler Kılavuzu", İstanbul, 1999.

Maliye Bakanlığı, "Kamu İç Kontrol Standartlarına Uyum Eylem Planı", 2010.

MAR Steve, JOHANNESSEN Rune, COATES Stephen, WEGRZYNOWİCZ Karine ve ANDREESEN Thomas. **GTAG (Global Technology Audit Guide)-Information Technology Risk and Controls**, 2 Edition, March 2012.

NALBANTOĞLU Rıfat T. "Türk Bankacılık Sektöründe Krediler ve Muhasebe Denetim Mesleği", **Muhasebe Denetimi Sempozyumu**, İstanbul, 2-6 Mayıs 2001.

ROT Artur. “IT Risk Assesment: Quantitative and Qualitative Approach”, **Proceedings of the World Congress on Engineering and Computer Science**, 22-24 Ekim 2008, San Francisco, USA.

SÜER Ayça Zeynep, “Profesyonel Muhasebe Mesleğinde Enron Skandalı ve Sonrası Gelişmeler”, **VI. Türkiye Muhasebe Denetimi Sempozyumu**, Antalya, 16-20 Nisan 2003.

TEKER Suat. “Aktif-Pasif Yönetimi”, T.B.B Eğitim Notları, İstanbul, 14-16 Şubat 2001.

The American Institute of Certified Public Accountants Auditing Guide nr.78.

The Orange Book “Management of Risk - Principles and Concepts”, HM Treasury, Norwich UK, 2004.

Türkiye Bankalar Birliği, “Bankalarda İç Denetim ve Bankacılık Gözetim Otoritesinin İç ve Dış Denetçiler İle İlişkisi”, **Bankacılık Gözetimine İlişkin Basel Komitesi Tarafından Yayımlanan Danışma Belgesi**, Temmuz 2000.

Türkiye Bankalar Birliği, “Finansal Kurumlar İçin Risk Değerlendirme Çerçevesi”, Ocak 2004.