T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
İÇ DENETİM VE RİSK YÖNETİMİ BİLİM DALI

YÜKSEK LİSANS TEZİ

BANKACILIKTA UYUM RİSKİ VE REGÜLASYON TEKNOLOJİSİ (REGTEK) UYGULAMALARI

Çağlar DÖNMEZ

2501200414

TEZ DANIŞMANI

Prof. Dr. Davut PEHLİVANLI

İSTANBUL – 2023

ÖZ

BANKACILIKTA UYUM RİSKİ VE REGÜLASYON TEKNOLOJİSİ (REGTEK) UYGULAMALARI

Çağlar DÖNMEZ

Kamu, özel, kâr amacı güden veya gütmeyen her kuruluş uyum riskine maruz kalmaktadır. Bir kuruluşun yasalara, yönetmeliklere, standartlara, iç politika ve prosedürlere uymamasından kaynaklanabilecek potansiyel kayıpları belirlemesi ve değerlendirmesi kurumun hem finansal kayıp hem de itibar kaybı yaşamaması için önemlidir. Özellikle 2008 finansal krizinden sonra düzenlemelerin yoğun olduğu bankacılık sektöründeki uyum riski yönetiminde teknolojinin daha fazla kullanılması ihtiyacı ortaya çıkmıştır.

Bankacılıktaki düzenlemelerin artması, teknolojik gelişmeler ve açık bankacılığın yaygınlaşmaya başlaması RegTech sektörünün büyümesine ve gelişmesine katkı sağlamıştır. Uyum, risk yönetimi, işlem izleme, yasal raporlama gibi çeşitli alanlarda çözümler üretilmesi uyum riski yönetimini kolaylaştırmış ve potansiyel kayıpları azaltmıştır.

Bu çalışmada bankacılık sektöründe uyum riski ve denetimi, RegTech çözümleri ve uyum riski yönetiminde kullanım alanları değerlendirilmiştir. Bununla birlikte uyum riskinin bankacılık sektörüne maliyeti, bankalara verilen çeşitli cezalar, proaktif uygulamalar ve Wells Fargo vakası incelenmiş olup RegTech çözümlerinin uyum riski yönetiminin ayrılmaz bir parçası olması gerektiği, verilen ceza örneklerine bakıldığında finansal kayıpları önleyebileceği ve gelecekte dijital bankacılıkla birlikte kullanım alanlarının artacağı ve daha da yaygınlaşacağı sonucuna varılmıştır.

Anahtar Kelimeler: RegTech, RegTek, Uyum, Uyum Riski, Risk, Risk Yönetimi, Uyum Riski Yönetimi, Uyum Riski Denetimi, Proaktif Uygulamalar, Uyum Maliyeti, Uyum Cezaları, Regülasyon, Dijital Bankacılık

ABSTRACT

COMPLIANCE RISK AND REGULATORY TECHNOLOGY (REGTECH) APPLICATIONS IN THE BANKING SECTOR

Çağlar DÖNMEZ

Public, private, for-profit or not, every organization is exposed to compliance risk. It is important for an organization to identify and evaluate potential losses that may arise from non-compliance with laws, regulations, standards, internal policies and procedures, so that the organization does not experience both financial and reputational loss. Especially after the 2008 financial crisis, the need to use technology more in compliance risk management in the banking sector, where regulations are intense, has emerged.

The increase in regulations in the banking sector, technological developments and the spread of open banking contributed to the growth and development of the RegTech sector. Developing solutions in various areas such as compliance, risk management, transaction monitoring and regulatory reporting has facilitated compliance risk management and reduced potential losses.

In this study, compliance risk and auditing in the banking sector, RegTech solutions and usage areas in compliance risk management are evaluated. In addition, the cost of compliance risk to the banking sector, various fines given to banks, proactive applications and the Wells Fargo case are examined. It has been concluded that RegTech solutions should be an integral part of compliance risk management, that they can prevent financial losses when looking at the examples of fines and that their usage areas will increase and become more widespread in the future with digital banking.

Keywords: RegTech, Compliance, Compliance Risk, Risk, Risk Management, Compliance Risk Management, Compliance Risk Audit, Proactive Applications, Cost of Compliance, Regulatory Cost, Compliance Fines, Regulation, Digital Banking

ÖNSÖZ

Bu çalışmada bankacılık sektöründeki uyum riski yönetimi ve denetimi, uyum riskinin yönetilmesinde ve denetlenmesinde kullanılan regülasyon teknolojilerinin (RegTech) etkisi, uyum riskinin bankacılık sektörüne maliyeti ve RegTech çözümleri çalışılmış olup bankalara verilen çeşitli cezalara ve RegTech firmalarına örnekler verilmiş ve Wells Fargo vakası incelenmiştir.

Çalışmanın tüm aşamalarında kıymetli görüş, öneri ve desteklerini esirgemeyen, karşılaştığım zorluklarda bana yol gösteren ve danışmanlığımı üstlenerek çalışmamı onurlandıran Prof. Dr. Davut Pehlivanlı'ya teşekkürlerimi sunarım.

Ayrıca sevgisini, güvenini ve desteğini hiçbir zaman esirgemeyen değerli eşim Sevim Yıldırım Dönmez'e, eğitim hayatımda bugüne gelmemde büyük emeği olan ve her daim beni destekleyen sevgili annem Vildan Dönmez ve sevgili babam Kemal Dönmez'e teşekkür ederim.

ÇAĞLAR DÖNMEZ

İSTANBUL, 2023

İÇİNDEKİLER

ÖZ ..... **II**
ABSTRACT ..... **III**
ÖNSÖZ ..... **IV**
TABLOLAR LİSTESİ ..... **VIII**
ŞEKİLLER LİSTESİ ..... **X**
KISALTMALAR LİSTESİ ..... **XI**
GİRİŞ **1**

BİRİNCİ BÖLÜM
KAVRAMSAL ÇERÇEVE

1. Kavramsal Çerçeve: RegTech, Uyum, Regülasyon ve Literatür Taraması ... 3
   1.1. RegTech Kavramı ... 3
      1.1.1. RegTech 1.0 ... 4
      1.1.2. RegTech 2.0 ... 4
      1.1.3. RegTech 3.0 ... 5
   1.2. Uyum Kavramı ... 6
   1.3. Regülasyon Kavramı ... 7
   1.4. Literatür Taraması ... 7
      1.4.1. Uyum Riski Konusunda ... 7
      1.4.2. RegTech Konusunda ... 8

İKİNCİ BÖLÜM
UYUM RİSKİ YÖNETİMİ VE DENETİMİ

2. Uyum Riski Yönetimi ve Denetimi ... 10
   2.1. Bankacılık Sektöründe Uyum Riski ... 10
      2.1.1. Uyum Riski Kavramı ... 10
      2.1.2. Kara Paranın Aklanması ve Terörizmin Finansmanı ... 11
      2.1.3. Diğer Mevzuata Uyum Faaliyetleri ... 14
   2.2. Bankacılık Sektöründe Uyum Riski Yönetimi ve Denetimi ... 16
      2.2.1. Müşteri Kabul Süreçlerinin Denetimi ... 22
      2.2.2. Risk Yönetimi Faaliyetlerinin Denetimi ... 24
      2.2.3. İzleme ve Kontrol Faaliyetlerinin Denetimi ... 25
      2.2.4. Şüpheli İşlem Bildirimleri Denetimi ... 26
      2.2.5. Oluşturulan Mevzuatın ve Yeni Ürünlerin Uygunluğunun Denetimi ... 27
      2.2.6. Eğitim Faaliyetlerinin Denetimi ... 28
      2.2.7. KVKK Denetimi ... 28

ÜÇÜNCÜ BÖLÜM
REGTECH EVRENİ VE BANKACLIKTA REGTECH

3. RegTech ve Bankacılık İlişkisi 30
3.1. RegTech 30
3.1.1. RegTech Ekosistemi 30
3.1.2. RegTech Fayda ve Zorlukları 33
3.1.3. RegTech Sektörünün Geleceği 35
3.2. RegTech Altyapısı 37
3.2.1. Yapay Zekâ 37
3.2.2. API 38
3.2.3. Büyük Veri 38
3.2.4. Blok zinciri 39
3.2.5. Akıllı Sözleşmeler 40
3.2.6. Nesnelerin İnterneti 41
3.2.7. Bulut Teknolojisi 42
3.2.8. Robotik Süreç Otomasyonu 43
3.3. RegTech Çözümleri 43
3.3.1. Uyum 44
3.3.2. Kimlik Yönetimi ve Kontrolü 44
3.3.3. Risk Yönetimi 45
3.3.4. Yasal Raporlama 46
3.3.5. İşlem İzleme 46
3.4. Dijital Bankacılık Çağı 47
3.4.1. Açık Bankacılık 47
3.4.2. Servis Bankacılığı 49
3.4.3. Neobankalar 50
3.4.4. Rekabetçi Bankalar 50
3.5. RegTech ve Bankacılık İlişkisi 51

DÖRDÜNCÜ BÖLÜM
UYGULAMADA REGTECH

4. RegTech Uygulamaları ve Wells Fargo Vaka İncelemesi 54
4.1. Uyum Maliyeti 54
4.2. Uyum Cezaları 59
4.3. Uyum Riskinde Proaktif Uygulamalar ve Wells Fargo Vakası 65
4.3.1. Bankacılıkta Operasyonel Risk 65
4.3.2. Uyum Riskinin Operasyonel Süreçler İçerisindeki Yeri ve Proaktif Uygulamalar 66
4.3.3. Wells Fargo Vakası 69
4.3.3.1. Bankanın Kısa Tarihi 69
4.3.3.2. Banka Satış Politikası 70

4.3.3.3. Skandalın Gelişimi 71
4.3.3.4. Çıkarılacak Sonuçlar 74
4.4. Bankacılıkta Uyum Riskine Yönelik RegTech Kullanım Alanları 75
4.4.1. RegTech Kullanım Alanları ve Firma Örnekleri 76
4.4.2. Türkiye Bankacılık Sistemine RegTech Çözümleri Entegrasyonu 79
4.4.3. Halkbank Vakası 83
4.4.3.1. Altın ve Gıda Yöntemi 84
4.4.3.2. Uyum ve Risk Değerlendirmesi 84
4.4.4. İç Denetimde RegTech Kullanım Alanları 85
SONUÇ 87
KAYNAKÇA 92

TABLOLAR LİSTESİ

Tablo 2.1 : Uyum Riskini Önleme Programının Bileşenleri (smaart)..... 18
Tablo 3.1 :Türkiye Açık Bankacılık Açık Kaynak API Listesi 49
Tablo 4.1 :Bölgelere Göre Mali Suçlarda Uyum Maliyeti..... 57
Tablo 4.2 : Banka Cezaları..... 61
Tablo 4.3 : Wells Fargo Teşvik Planları Karşılaştırması 73
Tablo 4.4 : Wells Fargo'ya Verilen Para Cezaları 74

GRAFİKLER LİSTESİ

Grafik 2.1 :Şüpheli İşlem Bildirimleri Yıllara Göre Dağılımı (2017-2021)..... 26
Grafik 3.1 :Yıllara Göre RegTech Yatırımları..... 33
Grafik 3.2 : RegTech Sektörü Büyüme Tahmini (milyar $)..... 36
Grafik 3.3 :2014-2022 Yılları Arasındaki Rekabetçi Bankaların Sermaye Fonlamaları 51
Grafik 4.1 : Tarihsel Olarak Yapılan Düzenlemeler..... 56
Grafik 4.2 :Yıllık Toplam Düzenleyici Yayın, Değişiklik ve Duyuru Sayısı 56
Grafik 4.3 : Rusya Savaşı Nedeniyle Avrupa Birliği Yaptırımlarının Kümülatif Sayısı..... 59
Grafik 4.4 : Global AML Kaynaklı Ceza Tutarları 61
Grafik 4.5 : Deloitte Araştırmasındaki Uygulamaların Zaman Tasarrufu Sağlama Oranları 76
Grafik 4.6 : Deloitte Araştırmasındaki Uygulamaların Maliyet Tasarrufu Sağlama Oranları 76
Grafik 4.7 : Deloitte Araştırmasındaki Uygulamaların Kullandığı Teknolojilerin Alanlarına Göre Oranı..... 77
Grafik 4.8 :Türkiye'de İdari Para Cezasına Konu Fiillerin Yıllar İtibarıyla Grafiksel Dağılımı 81

ŞEKİLLER LİSTESİ

Şekil 2.1 :İç Denetim ve Risk Yönetim Sistemi 14
Şekil 2.2 :IIA'nin Üçlü Hat Modeli 21
Şekil 3.1 : RegTech Ekosistemi 31
Şekil 3.2 : RegTech Sektör Haritası 32
Şekil 3.3 : Geleneksel Bankacılık ve Açık Bankacılık Modelleri 48

KISALTMALAR LİSTESİ

ABD **:** Amerika Birleşik Devletleri
AG **:**Aktiengesellschaft
AI **:**Artificial intelligence
AIFMD **:**Alternative Investment Fund Managers Directive
AML **:**Anti-Money Laundering
API **:**Application Programming Interface
ATM **:**Automated Teller Machine
AUS **:**Australia
B2B **:**Business to Business
B2C **:**Business to Consumer
Baas **:**Banking-as-a-Service
BaFin **:**Federal Financial Supervisory Authority
BCBS **:**Basel Committee On Banking Supervision
BDDK **:**Bankacılık Düzenleme ve Denetleme Kurumu
BIS **:**Bank of International Settlements
BoE **:**The Bank of England
BT **:**Bilgi Teknolojileri
CBDC **:**Central Bank Digital Currency
CEO **:**Chief Executive Officer
CFPB **:**Consumer Financial Protection Bureau
CFT **:**Combating the Financing of Terrorism
CFTC **:**Commodity Futures Trading Commission
CMA **:**Competition and Markets Authority
CRD **:**Capital Requirements Directives
DeFi **:**Decentralized Finance
DLT **:**Distributed Ledger Technology
EBA **:**European Banking Authority
EMIR **:**The European Market Infrastructure Regulation
EURIBOR **:**Euro Inter Bank Offered Rate
FATCA **:**Foreign Account Tax Compliance Act

FATF **:**Financial Action Task Force

FCA **:**Financial Conduct Authority

FED **:**The Federal Reserve System

FinTech **:**Financial Technology

FOFA **:**Future of Financial Advice

GDPR **:**General Data Protection Regulation

GRC **:**Governance, Risk, and Compliance

G-SIB **:**Global Systemically Important Banks

IaaS **:**Infrastructure as a Service

IDV **:**Identity Verification

IIA **:**The Institute of Internal Auditors

IoT **:**Internet of Things

IPA **:**Intelligent Process Automation

KVKK **:**Kişisel Verilerin Korunması Kanunu

KYB **:**Know Your Business

KYC **:**Know Your Customer

LGT Bank **:**Liechtenstein Global Trust Bank

MAR **:**The Market Abuse Regulation

MAR **:**The Market Abuse Directive

MASAK **:**Mali Suçları Araştırma Kurulu

MiFID **:**Markets in Financial Instruments Directive

NFC **:**Near Field Communication

NIOC **:**National Iranian Oil Company

NLP **:**Natural Language Processing

OCC **:**Office of the Comptroller of the Currency

OCR **:**Optical Character Recognition

OFAC **:**The Treasury Department's Office of Foreign Assets Control

OTP **:**One-Time Password

PaaS **:**Platform as a Service

POS **:**Point of Sale

PSD **:**Payment Services Directive

QR **:**Quick Response

RegTech **:**Regulatory Technologies

RegTek **:**Regülasyon Teknolojileri

RPA **:**Robotic Process Automation

SaaS **:**Software as a Service

SEC **:**Securities and Exchange Commission

SGA/TF **:**Suç Gelirlerinin Aklanması/Terörizmin Finansmanı

Smaart **:**Systems-Monitoring-Assessment-Accountability-Response-Training

SMS **:**Short Message Service

SOX **:**Sarbanes–Oxley Act

SupTech **:**Supervisory Technology

TBB **:**Türkiye Bankalar Birliği

TCMB **:**Türkiye Cumhuriyet Merkez Bankası

TDK **:**Türk Dil Kurumu

TILA **:**The Truth in Lending Act

RESPA **:** The Real Estate Settlement Procedures Act

UBS **:**Union Bank of Switzerland

UCITS **:**Undertakings for the Collective Investment in Transferable Securities

UK **:**United Kingdom

US **:**United States

VP Bank **:**Verwaltungs und Privat Bank

GİRİŞ

2008 küresel finans krizi, küresel ekonominin altında yatan sistemik risklerin yanı sıra özellikle ABD'de ve Avrupa ülkelerinde finansal piyasa düzenlemelerinin ne kadar yetersiz olduğunu ortaya çıkarmıştır. Küresel kriz sonucunda gözetim mekanizmalarının güçlenmesi, kurum ve firmaların uyması gereken düzenlemelerin her geçen gün artması, ülke ekonomilerinin küreselleşmesi ve teknolojinin gelişmesiyle birlikte işlem adet ve hacimlerinin artması gibi nedenlerle finansal kurumlar karmaşık ve maliyetli bir uyum süreci ile karşı karşıya kalmıştır. Bu nedenle günümüzde finansal kurumlardaki uyum riski yönetimi önem kazanmaya başlamıştır.

Geçmişte uyum riskini ele almak daha kolay iken günümüzde yasal düzenlemelerin artmasıyla birlikte daha karmaşık hale gelmiştir. Bu nedenle finansal kurumlar uyum riski yönetimi için daha fazla kaynak ayırmak zorunda kalmaktadır.

Uyum riski yönetimi, finansal piyasaların ana aktörlerinden biri olan bankalar için önemi büyüktür. Bankacılık sektöründeki düzenlemelerin fazla olması, kara para aklanmasının önlenmesi ve müşterini tanı gibi dinamik yönetilmesi gereken süreçlerin bulunması bankacılık sektöründeki uyum riskinin yönetilmesini önemli hale getirmektedir. Ayrıca bankacılık sektöründe dijital bankacılık, açık bankacılık ve servis bankacılığı alanlarında yaşanan gelişmeler bankacılıkta uyum riskini artırmıştır. Böylece uyum riski yönetimindeki artan maliyetler ise kurumların teknolojik çözüm arayışı içine girmelerini sağlamıştır.

Uyum riski yönetimindeki teknolojik çözümlerden biri 'Regulatory Technology' kısa adıyla RegTech'tir. RegTech firmaları, finansal kurumların uyumluluk standartlarını karşılamalarına, risk yönetimi protokollerinin yürürlükte olduğundan emin olmalarına ve riski proaktif bir şekilde azaltan kontrolleri uygulamaya koymalarına yardımcı olmaktadır. Bu teknoloji, mevcut uyumluluk, denetim ve risk iş akışlarını tamamlamaktan, yapay zeka, makine öğrenimi ve blok zinciri gibi en son teknolojilerden yararlanarak bunları değiştirmeye ve tamamen otomatikleştirmeye kadar uzanmaktadır. Teknolojik gelişmelerin yanısıra açık bankacılık alanındaki gelişmeler de RegTech sektörünü etkilemiş ve sektörün büyümesine ve gelişmesine katkı sağlamıştır.

Bu kapsamda çalışmanın amacı; küresel olarak artan düzenlemelerin getirdiği zorlukların aşılması için bankaların uyum riski yönetiminde gelişen teknolojilerin kullanımına ilişkin değerlendirmelerin yapılması ve söz konusu teknolojilerin uyum riski denetimine etkisinin incelenmesidir. Amaç doğrultusunda çalışmanın birinci bölümünde uyum riski ve RegTech hakkında temel bilgiler verilecek, ikinci bölümünde uyum riski yönetiminin bankacılık sektöründeki yeri ve denetime etkisi incelenecek, üçüncü bölümde RegTech'ler hakkında daha detaylı incelemeler yapılarak bankacılık ile ilişkisi değerlendirilecek, dördüncü bölümde ise uyum maliyeti, uyum cezaları ve RegTech kullanım alanları incelenerek RegTech firmalarından örnekler verilecek ve Wells Fargo vakası değerlendirilerek çalışma tamamlanacaktır. Böylece RegTech'lerin uyum riski denetim konularında bankacılık sektörüne etkisi ve uygulama alanlarının neler olduğu sorusuna yanıt aranmış olacaktır.

BİRİNCİ BÖLÜM
KAVRAMSAL ÇERÇEVE

1. Kavramsal Çerçeve: RegTech, Uyum, Regülasyon ve Literatür Taraması

Regülasyon veya düzenleme, bir otorite tarafından oluşturulan ve uygulanan kurallar bütünüdür. Bu kurallara uyulmaması durumunda yasal otoritelerin uygulayacağı cezalar neticesinde paydaşlar açısından potansiyel zarar kaybı meydana gelebilir. Bu kayıpların yaşanmaması için de uyum riski yönetiminde RegTech araçları kullanılmaktadır. Çalışmanın bu bölümünde RegTech, uyum ve regülasyon kavramları açıklanmış, uyum riski ve RegTech konularında literatürde hangi çalışmaların yer aldığı incelenmiştir.

1.1. RegTech Kavramı

RegTek (RegTech) kavramı literatürde İngilizce karşılıkları olan "regulatory" ve "technology" yani "regülasyon" ve "teknoloji" kavramlarının kısaltmalarının birlikte kullanılmasıyla oluşturulmuş bir kelimedir. Düzenleyici teknoloji ya da kısa adıyla RegTech, finansal piyasalarda yapılan düzenlemelere uyum süreçlerini iyileştirmek için düzenleyici izleme, raporlama ve uyum bağlamında teknolojinin yoğun olarak kullanıldığı çözümleri ifade etmektedir (Arner, v.d., 2016a: 81). Diğer bir tanımda ise düzenleme ve uyumluluk gereksinimlerini daha etkin ve verimli bir şekilde çözmek için yeni teknolojilerin kullanılması olarak belirtilmiştir (Institute of International Finance, 2015: 2).

RegTech, hem regülasyon sorunlarıyla başa çıkmada firmalara yardımcı olmayı amaçlayan teknolojik çözümleri hem de bu iş alanında uzmanlaşmış firma veya kuruluşları tanımlamak için kullanılmaktadır. RegTech'lerin amacı yeni düzenlemelere ve manuel raporlamaya yardımcı olmaktır. Ayrıca risk değerlendirmesi ve yönetimi, kimlik yönetimi ve kontrolü, işlem izleme, veri yapılandırma ve kara para aklamanın önlenmesi (AML) gibi alanlarda çözüm sunmaktadır (Deloitte, 2017a: 4; Yang ve Li, 2018: 3268).

RegTech'lerin olası faydaları, daha düşük maliyetli olması, etkin ve verimli uyum süreçleri, gerçek zamanlı veri elde edilmesi, doğru bilgiye kolay erişim, kolay raporlama ve güvenliktir (Hill, 2018). Ayrıca RegTech bulut teknolojisi, blok zincir, makine öğrenimi, büyük veri, veri madenciliği gibi teknolojik altyapıları çözmeye çalıştığı soruna bağlı olarak kullanmaktadır (Deloitte, 2017b: 75).

RegTech'in gelişimi üç aşamada kategorize edilmiştir: RegTech 1.0, RegTech 2.0 ve RegTech 3.0 (Arner, v.d., 2017:10; KPMG, 2018: 6). RegTech 1.0, 1990'larda başlayan ve 2008'den önceki zamanı ifade eden, risk yönetimi ve izlemeye odaklanan teknolojik çözümlere atıfta bulunan dönemi ifade eder. RegTech 2.0, 2008 küresel mali kriz ile finansal piyasalardaki düzenlemelerin arttığı, bunun da firmaların uyum maliyetini ve karmaşıklığı artırdığı günümüz dönemini ifade etmektedir. RegTech 3.0 ise dijitalleşmenin arttığı ve buna bağlı olarak dijital varlıkların çeşitlendiği, farklı teknolojilerin araç olarak kullanılarak çözümler geliştirildiği henüz tamamlanmamış dönemi ifade etmektedir.

1.1.1. RegTech 1.0

RegTech 1.0 olarak adlandırılan bu dönem, bilgisayar teknolojilerinin geleneksel finans kurumları tarafından kullanılmaya başlandığı 1990 ve 2008 yılları arasını kapsamaktadır. Bu dönemde kurumların küreselleştikçe artan düzenleyici zorluklarla karşı karşıya kalmaları, kendi uyum ve risk yönetimi departmanlarını kurmalarına yol açmıştır (Fineksus / Fintech İstanbul, 2020: 11). Finansal teknolojilere benzer teknolojileri de bu departmanlarda kullanan finansal kurumlar, risk yönetimini kolaylaştırmaya çalışmışlardır. Yeni teknolojilerin risk yönetimine uygulanmaya başlandığı ve sistemin güvenilir olmasına dayanan bu dönem 2008 küresel mali krizi ile sona ermiştir (Arner, v.d., 2017: 8).

1.1.2. RegTech 2.0

RegTech 2.0 olarak adlandırılan bu dönem 2008 küresel mali krizinden sonra düzenlemelerin artması ve firmaların uyum süreçlerindeki ihtiyaçlar nedeniyle ortaya çıkmış bir dönemdir. Sürekli yapılan düzenlemeler karmaşıklığa neden olmuş, uyum maliyetlerini önemli ölçüde artırmış ve buna bağlı olarak yasal para cezaları da önemli ölçüde artmıştır (Fineksus / Fintech İstanbul, 2020: 12).

Bu dönemde güçler ayrılığı ilkesini uygulayabilmek için ulusal ve uluslararası boyutta yeni yasal yapılar ve yasal yapılarda bölünmeler meydana gelmiştir. Örneğin, bankacılık alanında BIS tarafından Basel III kriterleri yayımlanmış, böylece bankalar kurumsal yönetişim ve risk yönetiminde kapsamlı değişikliklere yol açan düzenlemelere maruz kalmışlardır.

Finansal kurumlar bu dönemde uyum süreçlerini geliştirmek için veriye dayalı bilgi toplama ve analiz etme konularında Yapay Zeka (AI), derin öğrenme gibi teknolojik çözümlerden daha yoğun bir şekilde faydalanmışlardır. Özellikle RegTech çözümleri olmadan Kara Parayı Aklamayı Önlemek (Anti-Money Laundering – AML) ve Müşterini Tanıma (Know Your Customer – KYC) gibi süreçlerin yönetimi günümüzde neredeyse imkansızdır (Fineksus / Fintech İstanbul, 2020: 12).

1.1.3. RegTech 3.0

RegTech 3.0 olarak adlandırılan bu dönem Fintech alanındaki gelişmelere paralel olarak veri madenciliği, büyük veri, veri analizi, merkeziyetsiz finans (Decentralized Finance – DeFi) gibi kavramların önem kazandığı, fiziksel temasa dayalı müşteri odaklı yaklaşımdan dijital kimliğin önem kazandığı ve uzaktan müşteri edinimi süreçlerinin yaygınlaştığı henüz tamamlanmamış bir dönemdir (Arner, v.d., 2016a: 85). Bu dönemde blokzinciri teknolojisi akıllı sözleşmeler ile birleşmiş, token yapıları ile varlıklar dijitalleşmeye ve Merkez Bankaları Dijital Para Birimleri (Central Bank Digital Currency – CBDC) ortaya çıkmaya başlamış, yapay zekâ uygulamaları, bulut bilişim teknolojisi, API uygulamaları, makine öğrenmesi gibi kavramlar öne çıkmıştır (Deloitte, 2018b: 5). Hayatımızda birçok şeyin dijitalleşmesi ile birlikte yeni süreçlerin ortaya çıkması, yasal düzenlemelerin artması, firmaların yeniliklere hızlı adapte olma istekleri gibi nedenlerle RegTech çözümlerine ihtiyaç gittikçe artmaktadır. Dolayısıyla bu dönem, Fintech gelişmeleri ile paralel şekilde diğer dönemlerden farklı olarak kendini daha hızlı ve sürekli yenileyen bir bakış açısına sahiptir.

1.2. Uyum Kavramı

Uyum, Türk Dil Kurumu sözlüğünde "*Bir bütünün parçaları arasında bulunan uygunluk, ahenk*" olarak tanımlanmıştır (TDK). Finans sektörünü bir bütün olarak kabul edersek uyum kavramını geniş anlamda "*sektördeki finansal aktörlerin faaliyetlerinin yasal düzenlemelere uygunluğunun sağlanması*" olarak tanımlayabiliriz.

Bankacılıkta uyum kavramı ise "*Bankanın gerçekleştirdiği veya gerçekleştirmeyi planladığı tüm faaliyetlerin ve yeni işlemler ile ürünlerin banka dışı ve içi tüm mevzuata ve bankacılık teamüllerine uygun bir şekilde yürütülmesini sağlamak amacıyla yürütülen kontrol faaliyetleri*" olarak tanımlanabilir (Resmi Gazete, 2012).

5549 sayılı "Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun" uyarınca T.C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu Başkanlığı (MASAK) tarafından çıkartılan "Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelik" ile birlikte bankalar (Resmi Gazete, 2021);

- Kurum politikası ve prosedürlerinin oluşturulması,
- Risk yönetimi faaliyetlerinin yürütülmesi,
- İzleme ve kontrol faaliyetlerinin yürütülmesi,
- Uyum görevlisi atanması ve uyum birimi oluşturulması,
- Eğitim faaliyetlerinin yürütülmesi,
- İç denetim faaliyetlerinin yürütülmesi

önlemlerinden oluşan "uyum programı" oluşturmak ile yükümlü tutulmuştur. İlgili yönetmelik ile bankalar uyum programını yürütmek için uyum görevlisine bağlı bir uyum birimi kurmak zorundadır. Genelde uyum kavramı bankacılıkta kara para aklama, terörün finansmanı gibi konularda ilgili mevzuat ile eş anlamlı kullanılmaktadır. Bu çalışmada da uyum kavramı "yasal düzenlemelere uyum" olarak geniş anlamda kullanılacaktır.

1.3. Regülasyon Kavramı

Düzen kelimesinin sözlük anlamı, "*Belli yöntem, ilke veya yasalara göre kurulmuş olan durum, uyum, nizam, sistem*"dir (TDK). Piyasaların düzenlemesi açısından bakıldığında literatürde teknik bir terim olan "regülasyon" kavramı kullanılmaktadır. Regülasyon, ekonomiye devlet müdahalesi veya belirli bir amaç için konulan bir dizi kural olarak tanımlanabilir (Oğuz, 2011: 16). Devletlerin Rusya ve İran örneklerinde olduğu gibi uyguladıkları ambargolar da bu perspektiften düşünülebilir.

Regülasyon kavramını düzenleme ve denetleme işlevleri ile ele alındığında belli bir faaliyet ile ilgili olarak oyunun kurallarının belirlenmesi (düzenleme) ve bu kurallara uyulması (denetleme) olarak tanımlanabilir (Tepe ve Ardıyok, 2004: 107). Başka bir görüşe göre ise regülasyon, piyasaların bir üst otorite yoluyla düzenlenmesi, denetlenmesi, yönetilmesi ve yönlendirilmesi faaliyetlerini içermektedir (Oğuz, 2011: 19). İktisadi regülasyonun amacı, mevcut piyasa katılımcıları arasında yeterli rekabeti yaratan kurallar oluşturarak piyasaların etkinliğini sağlamaktır (Tepe ve Ardıyok, 2004: 108).

1.4. Literatür Taraması

Literatürde uyum riski ve RegTech konularında yer alan çalışmalar ayrı başlıklar altında incelenmiştir.

1.4.1. Uyum Riski Konusunda

Literatüre bakıldığında uyum riski değerlendirmesinin birkaç şekilde yapıldığı görülmektedir. Ludwick (2006) ve Birindelli & Feretti (2008) olayların meydana gelme olasılığı ve meydana gelmeleri halinde sonuçları açısından, Haynes (2005) etki eden faktörleri dikkate alarak ve Losiewicz- Dniestrzanska (2015) risk faktörlerinin derecelendirilmesi ve risk olasılığı açısından değerlendirmiştir. Asenov (2015), bankalar için uyum risklerinin belirlenmesi ve değerlendirilmesini incelerken, müşteri şikayetlerinin sayısı, nakit ödemelerin miktarı, bankaların yürürlükteki yasalara uymaması nedeniyle tespit edilen ihlallerin sayısı ve sıklığı gibi göstergelerin uygulanmasını önermektedir. Nicolas ve May (2017) uyum riskini değerlendirmek için denetim bulgularının, dış denetim ve süreç testleri sonuçlarından elde edilen

verilerin ve müşteri bilgilerinin dikkate alınmasını gerekli görmektedir. Ernst & Young (2021)'a göre, bankaların uyum işlevi, yasalara uygunluk, mali suçlar ile mücadele, veri gizliliği, siber güvenlik, operasyonel faaliyetler ve üçüncü taraf riski gibi ana alanları kapsamaktadır. Bazı alanlar ise kara para aklama, terörün finansmanı ve kitle imha silahlarının yayılmasının önlenmesi gibi alanlardaki riskler ile karakterize edilir.

Gabbi v.d. (2011), yabancı sermayeli finansal arabulucuların uyum risklerini değerlendirme ve tehlikelerini fark etme becerileri açısından daha deneyimli göründüğüne dikkat çekmiştir. Ayrıca Gabbi v.d. (2011), finansal kuruluşun faaliyetinin kapsamı (büyüklüğü) ile buradaki etkin uyum riski yönetimi arasındaki ilişkiyi tanımlamıştır. Arasa ve Ottichilo'ya (2015) göre, küçük kurumlar gelirleri sınırlı olduğu için KYC (Müşterini Tanı) gerekliliklerine uyum konusundaki giderleri karşılayamamaktadır. Dahl v.d. (2016), aynı konuyu küçük ve büyük bankalar için karşılaştırırken uyum maliyetlerini değerlendirmiş ve daha küçük bankaların daha büyük harcamalar yaptığı sonucuna varmıştır. Lagzdins ve Sloka (2012), Letonya bankaları ile ilgili çalışmasında uyum sistemlerinin değerlendirilmesini ve uyum programlarının uygulanmasını gözden geçirmiştir. Çalışmanın ardından yazarlar, özellikle küçük ve orta ölçekli bankaların organizasyonel iyileştirme ihtiyacını tanımlayan bir program konseptine sahip olmadığı sonucuna varmıştır.

1.4.2. RegTech Konusunda

Uyum ve RegTech konuları ile ilgili çalışmaları bulunan Avrupa Bankacılık Otoritesi (EBA)'nin AB finans sektöründe yasal raporlama gerekliliklerine uyum maliyetine ilişkin yaptığı RegTech analizi 2021 yılında tamamlanmıştır. Analizde özellikle küçük ve karmaşık olmayan düzenlemeye tabi kurumlar için raporlama maliyetlerinin %15-24 oranında azaltılması için öneriler sunulması amaçlanmış ve raporlama süreçlerinde teknolojinin daha geniş kullanımı teşvik edilmiştir (EBA, 2021a). EBA ayrıca regülasyon süreçlerinde gelişmiş teknolojik yeniliklerin düşünülmesine yönelik ek bir adım olarak kredi riski için düzenleyici sermayenin hesaplanmasında iç derecelendirmeye dayalı modeller için makine öğrenimi (Machine Learning) hakkında bir tartışma belgesi yayınlamıştır (EBA, 2021b).

EBA'nın diğer bir çalışması incelendiğinde, EBA açısından RegTech çözümlerinin uyumlaştırılması "izle, değerlendir ve uyarla" yaklaşımıyla sağlanabilir (EBA, 2021a: 78). Çalışmadaki uzun vadeli öneriler ise RegTech çözümlerinin merkezi bir AB veri tabanının oluşturulması ve sağlayıcıların RegTech çözümlerinin sertifikalandırılması olarak belirtilmiştir (EBA, 2021a: 79).

Gerçek zamanlı ve şeffaf bir düzenleyici sistem oluşturmaya katkıda bulunmak için RegTech'in olası sorunlar üzerine etkisi bir grup araştırmacı tarafından kaleme alınmıştır. Michaels ve Homer (2018) ve Buckley v.d. (2020) verideki bolluğun ve teknolojideki gelişimin teknoloji liderliğindeki veri odaklı denetimi teşvik edebileceğini ve risk odaklı düzenleyici yaklaşım sağlayabileceğini öne sürmüşlerdir. Kurum (2020), yenilikçi teknolojilerin uyum amacıyla güvenli bir şekilde nasıl kullanılacağını test etme ve öğrenme konusunda düzenleyici sanal alanların (sandboxes) yararlılığını araştırmıştır. Micheler ve Whaley (2020), strateji seçiminin kontrol ve özgürlük arasında olduğu kendi kendini düzenleme yaklaşımı (self-regulatory approach) veya meta-düzenleme gibi RegTech'in finansal düzenleme için çeşitli düzenleyici stratejilere nasıl entegre edilebileceğini tartışmıştır.

Hayır kurumlarına bağış toplama konusunda AML-CFT üzerine yapılan bir çalışmada, yapay zekâ, RegTech ve Charity Tech'in hayır kurumlarındaki düzenlemelere uyma, riski azaltma, kara para aklama ve terörün finansmanı ile ilgili olanlar da dahil olmak üzere suçla mücadele etme konularında yardımcı olabileceği belirtilmiştir (Singh ve Lin, 2020: 475-476). Aynı çalışmada hızlı otomasyon, gelişmiş istatistiksel modelleme, makine öğrenimi tabanlı risk analizi ve değerlendirme süreçlerinin, yaygın olarak uygulanan manuel süreçlerden çok daha etkili bir performansa sahip olduğu tespit edilmiştir (Singh ve Lin, 2020: 475-476).

RegTech 3.0 dönemindeki teknolojik gelişmelerin yeni olması nedeniyle literatürde çok fazla çalışma bulunmamaktadır. Daha fazla RegTech uygulaması ortaya çıktıkça ve veriler erişilebilir hale geldikçe, akademik literatürün muhtemelen daha nicel metodolojileri benimseyen belirli uygulamalara odaklanması beklenmektedir.

İKİNCİ BÖLÜM
UYUM RİSKİ YÖNETİMİ VE DENETİMİ

2. Uyum Riski Yönetimi ve Denetimi

Uyum riski, düzenlemelere uyulmaması durumunda firmaların karşı karşıya kalacağı itibar ve finansal kayıpları içinde barındırır. Uyum riskinin etkin yönetimi ile sektörde yer alan paydaşlar nezdinde güven sağlanır, itibar korunmuş olur ve ceza riski en aza indirilerek finansal fayda sağlanmış olur. Çalışmanın bu bölümünde bankacılık sektöründe uyum riski incelenmiş ve uyum riski bulunan alanlar ile ilgili denetim metodolojisi ele alınmıştır.

2.1. Bankacılık Sektöründe Uyum Riski

Bankaların çeşitli risklere karşı daha fazla kırılgan olmasının en önemli nedenleri; bankacılık yönetiminin artan karmaşıklığı, müşteri güvenini koruma ihtiyacı, kanunların ve davranış kurallarının zaman içinde artan ağırlığı olarak gösterilebilir. Son yıllarda başta itibar riski, uyum riski ve operasyonel riskler olmak üzere kredi ve piyasa risklerinden farklı risklerin, finansal kurumların istikrarı ve güvenilirliği için her zamankinden daha önemli olduğu anlaşılmıştır.

Bankacılık sektöründe uyum riski hem ulusal hem de uluslararası alandaki yasal otoritelerce yönetilmesi istenen, bankanın birçok iş sürecini etkileyen risklerden biridir. İlgili mevzuatlara bakıldığında bankacılıkta uyum riski genellikle suç gelirlerinin aklanmasının ve terörizmin finansmanının önlenmesi gibi konular ile ilgilidir. Bu bölümde uyum riski kavramı, uyum riskinin genel olarak kullanıldığı alanlar ve geniş anlamda kullanım alanları incelenmiştir.

2.1.1. Uyum Riski Kavramı

Uyum riski, Basel Komitesi tarafından "*Uyum riski, bir bankanın kanunlara, düzenlemelere, kurallara, ilgili öz düzenleyici kuruluş standartlarına ve bankacılık faaliyetleri için geçerli olan davranış kurallarına uymamasının bir sonucu olarak maruz kalabileceği yasal veya düzenleyici yaptırımların maddi mali kayıp veya itibar kaybı riski*" olarak tanımlanmıştır (BCBS, 2005: 7).

Bir banka, kendi risk yönetimi stratejisi ve yapısıyla tutarlı bir şekilde uyum riskinin yönetimi için öncelikler belirlemeli ve uyum fonksiyonunu düzenlemelidir. Örneğin, uyum riski ile operasyonel riskin belirli yönleri arasında yakın bir ilişki olduğundan, bazı bankalar uyum fonksiyonlarını operasyonel risk fonksiyonları içinde düzenlemek istemektedir. Bazı bankalar ise ayrı bir uyum ve operasyonel risk fonksiyonlarına sahip olmayı tercih etmekte ve uyum konusunda iki fonksiyon arasında yakın iş birliği gerektiren mekanizmalar kurmaktadır (BCBS, 2005: 8).

Uyum riski bankalarda hem iç hem de dış kaynaklı olabilir. İç faktörlere örnek olarak;

- Bankaların yürürlükteki mevzuatın gerekliliklerini yerine getirememesi,
- Bankaların iç mevzuatları ile yasal mevzuatlar arasındaki uyumsuzluk,
- Bankaların iç mevzuatlarını yasal mevzuatlara hızlı bir şekilde uyarlayamaması,
- Bankaların taraf olduğu sözleşmelere aykırılık,
- Çalışanların veya yönetimin eylemlerinden kaynaklanan hatalar

gösterilebilir. Dış faktörlere örnek ise;

- İlgili ülkenin hukuk sisteminin kusurlu olması (yasal düzenlemenin olmaması, uluslararası hukukun yanlış uygulanması vb.)
- Banka müşterilerinin veya karşı taraf ile yapılan sözleşmelerin ihlal edilmesi,
- Bankaların, şubelerinin veya bağlı ortaklıklarının farklı ülkelerin yetkisi altında olması

gösterilebilir.

2.1.2. Kara Paranın Aklanması ve Terörizmin Finansmanı

Paranın çeşitli renk sıfatları ile birlikte kullanılması, paranın kaynağını ifade etmektedir. Genel kabul görmüş ifade ile beyaz para yasal yollardan kazanılan ve vergisi verilen kazanç, gri para yasal yollardan kazanılan fakat vergiden kaçınılan ve kayıt dışına çıkan kazanç, kara para ise yasa dışı yollardan elde edilen kazançtır (Karaduman,2013: 4).

Kara para, *"yasaların suç saydığı eylemlerin işlenmesi suretiyle elde edilen bütün mal ve gelirleri, kara para aklama ise bu mal ve gelirlerin yasal bir kaynaktan elde edilmiş gibi gösterilmesine yönelik faaliyetleri"* olarak ifade edilmektedir (Üstün, 2016: 4). Terörizmin finansmanında ise yasadışı faaliyetlerden elde edilen kazançlar ile yasal faaliyetlerden elde edilen kazançların terör finansmanında kullanılması söz konusudur. İngilizcede kara para ile mücadele için "Anti-Money Laundering" (AML), terörizmin finansmanının önlenmesi için ise "Combating the Financing of Terrorism" (CFT) terimleri kullanılmaktadır.

Yasadışı yollar ile elde edilen kazançların finansal sisteme entegre edilip aklanması için kara para aklayanlar bu kazançları çeşitli aşamalardan geçirmektedir. Bunlar yerleştirme (placement), ayrıştırma (layering) ve bütünleştirme (Integration) aşamalarıdır (Nsundano, 2007: 1). Yerleştirme aşamasında para küçük parçalara ayrılarak finansal yapı içine veya perakendeye yerleştirilerek çeşitli varlıklara ayrılır ve farklı kişilere gönderilir. Ayrıştırma aşamasında kara paranın takibini zorlaştırmak ve kaynağından uzaklaştırmak amacıyla kısa süre içinde birden fazla karmaşık işlemler yapılır. Bütünleştirme aşamasında ise kara paranın ekonomiye tam entegre edilme evresidir. Bu evrede para aklayıcı bu parayla gayrimenkul, hisse senedi, tahvil, hazine bonosu vb. satın alarak parayı ekonomiye entegre eder (Mavral, 2001: 57).

Kara para aklama yöntemlerine bakıldığında çok sayıda kişi adına yasal mevzuatın belirttiği tutarın altındaki tutarlar ile banka hesaplarına para yatırılması yöntemi olan şirinler (smurfing) yöntemi; büyük miktardaki paranın parçalanarak az sayıda kişiye yatırılması yöntemi olan parçalama (structuring) yöntemi; gelirin kaynağının araştırılmadığı ülkelerdeki kıyı bankacılığı yapan bankalara paraların aktarılması; satış gelirlerinin tespit edilmesi zor sektörlerde göstermelik firmalar kurularak veya kağıt üzerinde paravan şirketler kurularak paranın aklanması; döviz büroları veya kumarhaneler yoluyla paranın aklanması gibi yöntemler kullanılmaktadır (Ergül, 2001: 35).

Günümüzde kara paranın aklanması ve bu paranın finansal sistem içerisine sokulması faaliyetlerinin büyük bir kısmı bankalar yoluyla yapılmaktadır. Bu nedenle bankaların uyum faaliyetleri ve denetimi kara para aklama ve terörün finansmanı ile mücadele konusunda önemli bir rol oynamaktadır. Finansal otoriteler bu risklerin

önlenmesinin ancak bankaların "müşterini tanı" prosedürlerini uygulayarak sağlanacağı kanısındadır. Bu konuda Mali Eylem Görev Gücü (Financial Action Task Force-FATF) ilk olarak 1990 yılında 40 Tavsiye Kararı yayınlamış ve daha sonraki yıllar revize etmiştir (FATF, t.y.).

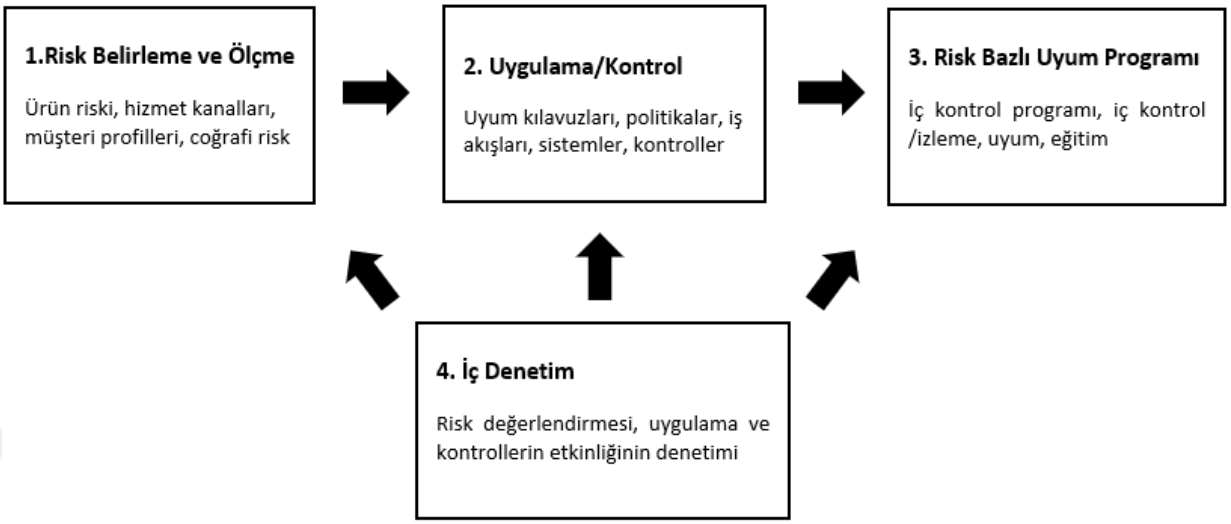
Tavsiyeye göre müşterini tanı ilkesinin getirdiği tedbirler;

- Kimlik tespiti yaparak bilgilerin güvenilirliğinden ve doğruluğundan emin olmak,
- Finansal işlem sonucunda nihai yararlanıcı olan kişinin kimliğini belirlemek,
- Tüzel kişiliklerde mülkiyetin kime ait olduğunu ve kim tarafından kontrol edildiğini belirlemek,
- Gerçekleştirilen finansal işlemin türünü ve yapılış amacını belirlemek,
- Yapılan işlemin takibini sağlamak

olarak özetlenebilir.

Türkiye'de bu konu ile mücadele hakkında 5549 Sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Kanunu 18 Ekim 2006 tarih ve 26323 Sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Kanuna göre Bankalar gerekli uyum ve tedbirleri alması gerekir. Bunlar; kimlik tespitinin yapılması, MASAK'a şüpheli işlem bildirimi yapılması, uyum programı oluşturularak uyum görevlisinin atanması ve istenildiğinde Başkanlık ve denetim elemanları tarafından istenilen her türlü bilgi, belge, kayıt ve şifrelerin verilmesi zorunluluğu olarak sıralanabilir.

Şekil 2.1: İç Denetim ve Risk Yönetim Sistemi



Kaynak: TBB-MASAK Çalışma Grubu, 2007: 61

Şekil 2.1'de gösterilen şemada suç gelirlerinin aklanmasının önlenmesine yönelik risk yönetim ve denetim sistemlerinin kurulmasına ilişkin;

1. Suç gelirlerinin aklanması ve terörizmin finansmanı konularındaki riskler belirlenir ve sayısallaştırılır,
2. İlgili risklerin yönetilmesi ve kontrol edilmesine ilişkin yazılı dokümanlar ve kontrol sistemi oluşturulur,
3. Süreklilik arz eden izleme faaliyetleri, iç kontrol, uyum ve personel eğitim programları hazırlanır,
4. Risk kontrol matrisleri hazırlanarak iş akışları ve kontrollerin etkinliğinin denetimi yapılır.

Bu sistemin uygulanmasındaki amaç bankaların ana bölümlere bağlı kalarak kendi prosedürlerini oluşturması, uygulaması ve kontrolünü sağlayarak değişen trendlere uyum sağlayan bir yapı inşa etmesidir (TBB-MASAK Çalışma Grubu, 2007: 62).

2.1.3. Diğer Mevzuata Uyum Faaliyetleri

Finansal sistem içinde hem bireyler hem de iş dünyası ve devletler açısından bakıldığında bankalar önemli aracı kuruluşlardan biridir. Bankaların finansal sistemin merkezinde yer almasından dolayı kriz zamanlarında en fazla etkilenen sektörlerden biri bankacılık sektörü olmuştur. Devletler krizleri tetikleyen nedenleri önlemek,

riskleri yönetmek ve sisteme müdahale etmek için bankacılık sektöründe düzenleme yapma gereği ortaya çıkmaktadır. Bankacılık sektöründe yapılan düzenlemeler sisteme müdahale edilebilmesi için ihtiyaçtan çok zorunluluk haline gelmiştir. Basel düzenlemeleri gibi uluslararası düzenlemelerin yanı sıra ülkeler kendi düzenlemelerini yaparak sektöre yön vermektedir. Ülkelerin gelişmişlik düzeylerine göre yapılan düzenlemeler de farklılık gösterebilir.

Sektörlere göre düzenlemeler "Düzenleyici ve Denetleyici Kuruluşlar" tarafından yapılır. Bu kuruluşlar; tüzel kişiliği ve karar organı bulunan, denetleme ve düzenleme görevini kanunlardan alan, idari ve mali açıdan özerkliğe sahip olan bağımsız kamu kurumlarıdır (Er, 2010: 183-184). Türkiye'de bankacılık sektörü BDDK (Bankacılık Düzenleme ve Denetleme Kurumu) tarafından düzenlenir ve denetlenir.

Türkiye'de banka ve işlemlerini doğrudan düzenleyen en güncel kanun 01.11.2005 tarih 5411 sayılı Bankacılık Kanunudur. Kanuna göre "*Bu Kanunda hüküm bulunmayan hallerde genel hükümler tatbik olunur.*" (Bankacılık Kanunu, Madde 2). Banka faaliyetleri birçok farklı sektör ve faaliyet alanı ile ilişkili olduğu için yapılan işlemlerin niteliğine göre diğer kanunlara da tabi olurlar. Medeni Kanun, Borçlar Kanunu, Türk Ticaret Kanunu, İcra ve İflas Kanunu gibi doğrudan bankacılık sektörünü düzenlemeyen kanunlar, Banka Kartları ve Kredi Kartları Kanunu, Çek Kanunu, Sermaye Piyasası Kanunu, Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun gibi bankaların çeşitli faaliyetlerine göre düzenlenen kanunlar örnek olarak gösterilebilir.

Kanunlarda açıkça düzenlenmeyen konular çeşitli yönetmelik, genelge, tebliğ, düzenleme, rehber ve kurul kararları ile düzenlenmektedir. Bunlara örnek vermek gerekirse (BDDK, t.y. ve TBB, t.y.);

- Dijital Bankaların Faaliyet Esasları ile Servis Modeli Bankacılığı Hakkında Yönetmelik
- Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik
- Tasarruf Mevduatı Sigorta Fonu Yönetmeliği

- Bankaların Kurumsal Yönetim İlkelerine İlişkin Yönetmelik
- Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik
- Bankaların Bağımsız Denetimi Hakkında Yönetmelik
- Kredilerin Sınıflandırılması ve Bunlar İçin Ayrılacak Karşılıklara İlişkin Usul ve Esaslar Hakkında Yönetmelik
- Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik
- Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Rapor Hakkında Tebliğ
- Konut Finansmanı Sözleşmeleri Yönetmeliği.

Diğer ülkelerdeki düzenlemelere baktığımızda 1970'li yıllardan sonra sermayenin serbest dolaşımı ile birlikte düzenlemeler ülkeden ülkeye farklılaşmaya başlamıştır. Bu farklılaşma da ülkeler arasında düzenleme arbitrajına neden olmaktadır. Sermaye düzenlemelerin daha zayıf olduğu ülkelere kaymaya başlamış ve bu ülkelerin avantajlı konuma geçmesini sağlamıştır (Tiryaki, 2010: 118). Bu nedenle ortak hareket etmek ve uzlaşma ortamı sağlamak amacıyla G10 ülkelerinin merkez bankalarının öncülüğünde 1974 yılında BIS (Bank of International Settlements) bünyesinde Basel Bankacılık Denetim Komitesi (Basel Committee On Banking Supervision- BCBS) kurulmuştur (BCBS, t.y. (a)). Komite, çeşitli alt komiteler ile bankacılık denetiminin kalitesini arttırma amacıyla çalışmalar yapmakta, banka faaliyetleri hakkında standartlar belirlemekte ve prensipler yayınlamaktadır (BCBS, t.y. (b)). Bankalar da günümüzde açıklanan Basel kriterlerine göre risklerini yönetmektedir.

2.2. Bankacılık Sektöründe Uyum Riski Yönetimi ve Denetimi

Uyum riski geçmişte sınırlı ve özel birkaç kurala dayandığı için daha kolay ele alınmıştır. Ekonominin küreselleşmesi, uluslararası firmaların ve bankaların uyması gereken yeni kuralların ortaya çıkmasına neden olmuştur. Ayrıca yeni krizlerin çıkması da bankacılık mevzuatının geniş çaplı değiştirilmesine ve yetersiz düzenlenmiş alanlara yönelik çalışma yapılmasına neden olmuştur. Amerika Birleşik Devletleri'nde Dodd-Frank Kanunu Düzenlemeleri (Dodd-Frank Wall Street Reform

and Consumer Protection Act), Yabancı Hesapların Vergi Uyumu Yasası (Foreign Account Tax Compliance Act -FATCA) ve Sarbanes-Oxley Yasası (Sarbanes–Oxley Act -SOX); Avrupa'da Basel III'ün getirdiği sermaye yeterlilik rasyosu, karşı taraf riskinin düzenlenmesi, kaldıraç oranı, sistematik risk kavramı ve likidite oranı gibi kriterler, Kişisel Verilerin Korunması Kanunu-KVKK(General Data Protection Regulation – GDPR), Finansal Araç Piyasaları Yönergesi (Markets in Financial Instruments Directive -MiFID) düzenlemeleri buna örnek gösterilebilir.

Basel kriterlerine baktığımızda uyum fonksiyonu bir banka içinde nasıl organize olursa olsun, yeterli kaynağa sahip olmalı, sorumlulukları açıkça belirtilmeli ve faaliyetleri, iç denetim fonksiyonu tarafından periyodik ve bağımsız incelemeye tabi tutulmalıdır (BCBS, 2005: 8-15). 2005 yılında uyum konusunda yayımlanan belgede uyumun temel görev ve sorumlulukları, uluslararası mali krize tepki olarak aşağıdaki gibi alanları kapsayacak şekilde genişlemiştir (BCBS, 2005: 13-14):

- Kara paranın aklanmasının ve terörün finansmanının önlenmesi,
- Çıkar çatışmalarının yönetilmesi,
- Piyasa suiistimali ve manipülasyonunun yasaklanması,
- Uyum konusunda personelin eğitilmesi,
- Bankanın faaliyetleriyle ilgili ortaya çıkan uyum risklerinin belirlenmesi ve değerlendirilmesi,
- Yıllık uyum planlarının hazırlanması,
- Uyum konusunda üst yönetime danışmanlık yapılması,
- Banka imajını geliştirilmesi ve itibarla ilgili risklerin ortadan kaldırılması,
- Banka performansının izlenmesi,
- İç kontrol ortamının geliştirilmesi ve buna uygun prosedürlerin oluşturulması,
- Üst yönetime düzenli olarak raporlama yapılması,
- Düzenleyici kurumlar ile iletişimin geliştirilmesi.

Uyum konusunda bankalara verilen cezalar parasal olarak maliyetli olmalarının yanı sıra banka itibarına da zarar vermektedir. Günümüzde bankalar itibarını koruma konusunda her zamankinden daha zorlu koşullar ile karşılaşmaktadır.

Bu zorlukların üstesinden gelmek için sürekli olarak iş süreçlerini iyileştirmeye ve risklerini daha etkin yönetmeye çalışmaktadır (Everson, v.d., 2003: 22).

Tablo 2.1 : Uyum Riskini Önleme Programının Bileşenleri (smaart)

(S) Systems Sistemler	İlgili düzenlemelere ve müşterinin gereksinimlerine uygun olarak işlemlerin hesap verebilirliğini sağlamak için prosedürlerin ve iç kontrolün uygulanması
(M) Monitoring İzleme	Banka program standartlarına uygun olarak sistemin gerçek zamanlı performansının sağlanması için Banka kontrol sisteminin işleyişi ile bağlantılı olarak günlük denetleme süreci
(A) Assessment Değerlendirme	İşlem ihlali ve program dezavantajını göstermek için özetlenmiş kayıtların ve işlemlerin periyodik analizi
(A) Accountability Hesap Verebilirlik	Banka düzenlemelerine uyum için politikaların uygulanmasına ve program sonuçları hakkında Banka yönetimine ve Yönetim Kurulu'na bilgi verilmesine yönelik personelin yönlendirilmesi için sorumluluk, yetki ve hesap verebilirliğin tahsis edilmesi
(R) Response Cevap	Müşteri şikayetlerinin işlenmesi, olağan şartlara aykırılıkların giderilmesi, kontrol prosedürlerinin değiştirilmesi, iç denetimdeki eksikliklerin düzeltilmesi ve politikaların, prosedürlerin uygulanması, bunların gözden geçirilmesi veya yenilenmesi
(T) Training Eğitim	Politikaya, prosedürlere, direktiflere, düzenleyicilerin gerekliliklerine uyum ilişkilerinde iletişim, personel eğitimi ve bilgileri dahil olmak üzere ürün ve hizmetlere ilişkin bilgiler

Kaynak: Asenov, 2015: 27

Uyum riskinin yönetim ve kontrol sistemi, diğer banka risklerinin kontrolüne benzemektedir. Sistemin gerekli kapasitesini sağlamak ve bazı açılardan faaliyetlerini finanse etmek (banka personelinin eğitimi gibi) pahalı olabilir fakat bu riskin ihmal edilmesi durumundaki kayıplar bazen bu riski önleme faaliyetlerinin maliyetinden daha fazla olabilmektedir. Düzenleyici ve denetleyici kurumlar tarafından bankaya verilecek bir ceza mali kayıpların yanında itibar kaybına da neden olacaktır. Bu sebeple uyum riskinin yönetimi itibar riski gibi diğer risklerin yönetimi için de önemlidir.

Bankalar uyum riskini yönetmek için hem düzenleyici kurumların dayattığı zorunluluk hem de kendi ihtiyaçları nedeniyle süreç bazlı çözümler geliştirir. Bankalarda uyum riskinin yönetimi genellikle aşağıdaki aşamalardan oluşur:

1. Uyum riskinin belirlenmesi;
2. Uyum riskinin değerlendirilmesi;
3. Uyum riskinin izlenmesi;

4. Uyum riskinin kontrol edilmesi ve en aza indirilmesi.

Bankalar uyum riskini yönetmek için mevzuat izleme ve uyum departmanlarını kurarak iş süreçlerini oluşturur. Bankanın uyması gereken düzenlemelere göre riskler belirlenir ve bu riskler olası etkilerine, gerçekleşme olasılıklarına ve önem derecesine göre önceliklendirilir ve değerlendirilir. Uyum riski yönetimi süreci sürekli olarak izlenerek yeterliliği ve etkinliği düzenli gözden geçirilir. Kontrol faaliyetleri ise bankanın uyum konusunda amaç ve hedeflerine ulaşabilmesi için riskin etki veya olasılığını düşürmeyi sağlayan eylemlerdir.

Uyum riski, iç denetim fonksiyonunun risk değerlendirme metodolojisine dahil edilmeli ve algılanan risk seviyesi ile orantılı kontrollerin test edilmesi de dahil olmak üzere bankanın uyum fonksiyonunun yeterliliğini ve etkinliğini kapsayan bir denetim programı oluşturulmalıdır (BCBS, 2005: 15).

Bu çalışmada kullanılan iç denetim kavramı 6 türü de kapsamaktadır. İlgili iç denetim türleri;

- Finansal denetim: Bir firmanın finansal tablolarının muhasebe ilkelerine ve yasal mevzuata göre gerçeğe uygunluğunun ve güvenilirliğinin kontrol edildiği denetim türüdür.
- Uygunluk denetimi: Bir firmanın faaliyetlerinin belirlenmiş kurallara ve mevzuata uygun olup olmadığının kontrol edildiği denetim türüdür (Güredin, 2008: 17).
- Faaliyet denetimi: Bir firmanın faaliyetlerinin firmanın belirlediği performans hedeflerine uygun olup olmadığı, etkinlik ve verimliliklerinin incelendiği denetim türüdür (Thornhill, 1981: 42).
- Bilgi teknolojileri denetimi: Bir firmanın kullandığı donanım, yazılım vb. bilgi teknolojilerinin güvenilirliğinin ve ne kadar sürdürülebilir olduğunun denetlendiği bir denetim türüdür (Kagermann, v.d., 2008: 118).
- Süreç denetimi: Bir firmanın süreçlerinin ne kadar etkin olduğu, faaliyetleri kapsayıp kapsamadığı, kontrol eksikliği olup olmadığı ve iç kontrol ortamının etkinliğinin denetlendiği bir denetim türüdür.

- Hile denetimi: Bir firmadaki çalışan veya yöneticilerin firmanın kaynaklarını kötüye kullanması, menfaat sağlaması veya kasıtlı olarak usulsüz işlemler yapması gibi faaliyetleri tespit etmek için yapılan denetim türüdür.

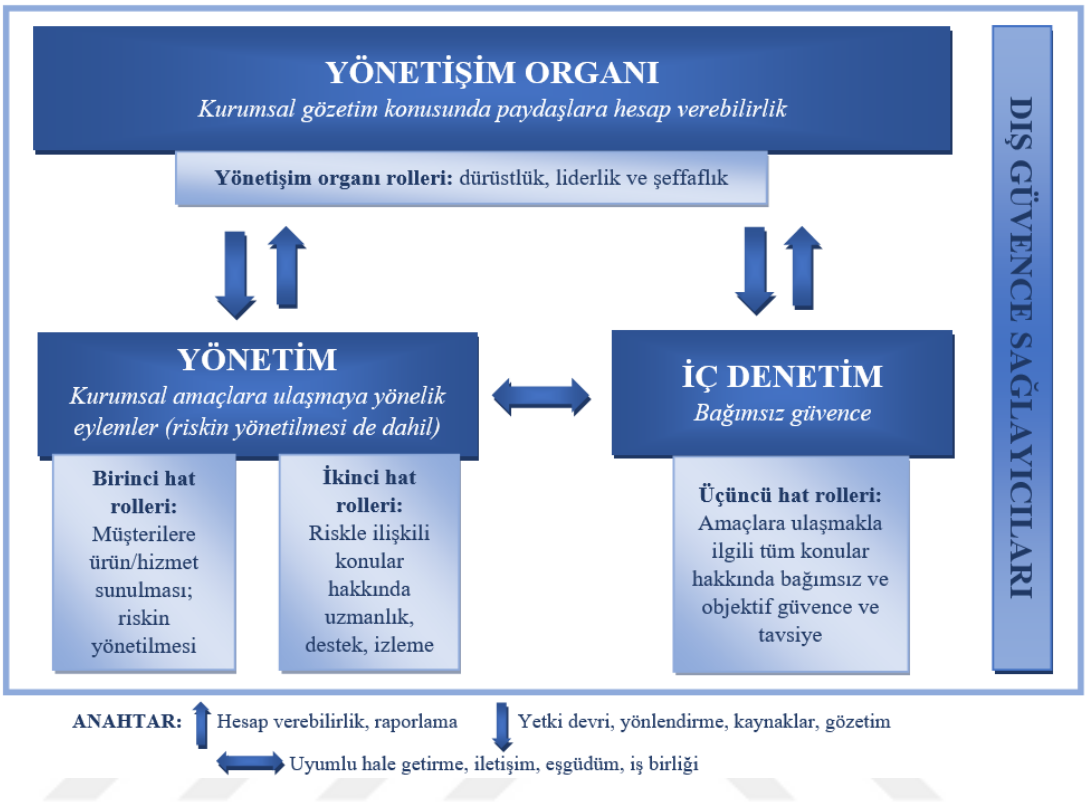
İç denetimin amacı, banka uyum programının bütününün etkinliği ve yeterliği hususunda bağlı olduğu yönetim kuruluna güvence sağlamaktır. Genel olarak müfettişlerce risk temelli incelenmesi ve denetlenmesi sağlanan unsurlara örnek olarak;

- Kurum politika ve prosedürlerinin, dış mevzuat içeriklerinde bulunan asgari unsurları karşılayıp karşılamadığı,
- Risk yönetimi, izleme ve kontrol faaliyetleri ile eğitim faaliyetlerinin etkin ve yeterli olup olmadığı,
- Banka birimlerinde yapılan işlemlerin SGA/TF mevzuatına ve banka içi politika ve prosedürlere uygun olarak yürütülüp yürütülmediği

gösterilebilir.

Bankalarda güçlü bir yönetişim ve risk yönetimi yapısı kurulması için kurumun amacına ulaşmasında yardımcı olacak yapı ve süreçlerin tanımlanmasında üçlü hat modeli kullanılmaktadır. Uluslararası İç Denetçiler Enstitüsü (The Institute of Internal Auditors-IIA)'nün ilk olarak Ocak 2013 tarihinde yayımladığı bu model uyum riski yönetimi ve denetiminde de yapı taşı olarak kullanılmaktadır.

Şekil 2.2 :IIA'nin Üçlü Hat Modeli



Kaynak: IIA, 2020: 4

Bankadaki birçok farklı grup, iş birimlerinden uyumluluk, denetim ve diğer risk yönetimi personeline kadar modelde belirgin bir rol oynamaktadır (Deloitte, t.y.(a)).

Birinci savunma hattında yönetim yani süreç sahipleri, günlük operasyonel faaliyetlerle ilgili riskleri sahiplenme ve yönetme konusunda birincil sorumluluğa sahiptir. Süreçteki Kontrollerin tasarımı, işletilmesi ve uygulanması bu savunma hattında üstlenilen diğer sorumluluklardandır.

İkinci savunma hattının işlevi, firmanın günlük işleyişinde ortaya çıkan risklerin tanımlanmasını sağlamaktır. Bunu da risk ve uyum yönetimini desteklemek için çeşitli politika, araç ve teknikler kullanarak uyum ve gözetim sağlayarak yapmaktadır.

Üçüncü savunma hattının işlevi, nesnel ve bağımsız güvence sağlamaktır. Üçüncü hattın temel sorumluluğu, birinci ve ikinci hat fonksiyonlarının etkin bir

şekilde çalışıp çalışmadığını değerlendirmek olmakla birlikte, düzenleyici kurumlara ve dış denetçilere güvence sağlamanın yanı sıra, kurul ve denetim komitesine raporlama yapmakla görevlidir.

2.2.1. Müşteri Kabul Süreçlerinin Denetimi

Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmeliğin üçüncü bölümünde "Müşterinin Tanınmasına İlişkin Esaslar" ayrıntılı olarak düzenlenmiştir. Müşteri tanı ilkesinin uygulanması Bankalarda kara para aklanmasının ve terörün finansmanın önlenmesi riskinin azaltılması hem ulusal hem de uluslararası alanda saygınlığının ve güvenilirliğinin artması için önemli bir yere sahiptir.

FATF, müşteri tanı ilkeleri ile ilgili 5 tavsiye tedbir açıklamıştır (Kalem ve Akın, 2009: 65).

Buna göre;

- Gerçek veya tüzel kişi müşterilerin kimlik bilgilerinin güvenilir belgeler ile teyit edilmesi
- Firma temsilcilerinin yetki durumlarının ve kimlik bilgilerinin teyit edilmesi
- Gerçekleştirilen veya gerçekleştirilecek işlemlerden faydalanacak kullanıcının kimlik bilgilerinin teyit edilmesi
- İş ilişkisi hakkında bilgi toplanması
- İş ilişkisi ile ilgili denetimin sürekli olması ve yapılan işlemlerin müşteri risk profili ile uyumluluğunun kontrol edilmesi

Finansal teknolojilerin gelişmesi ile Bankaların müşteri kabul süreçlerinde de değişiklik olmuştur. BDDK'nın 1 Nisan 2021 tarihinde çıkardığı "Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik" ile birlikte yeni müşteri kazanımı için uzaktan müşteri edinimi (Digital Onboarding) ve müşteri kimliğinin doğrulanması için uzaktan kimlik tespiti imkânı gelmiştir. Uzaktan Müşteri Edinimi dört temel süreçten ve bileşenden oluşmaktadır (Fineksus / Fintech İstanbul, 2020: 19);

- İlk Katılım (Onboarding): müşterinin kimliğini ilk başvurduğunda doğrulaması
- Doğrulama (Validation): müşterinin adres kontrolü, kredi puanı gibi bilgiler için doğrulama yapması
- Yetkilendirme (Authentication): müşterinin servis ve hizmetlere ulaşabilmesi için kimliğini doğrulaması
- Elektronik imzalama (Electronic signing): müşterinin sözleşmelerini yasal olarak geçerli olacak şekilde dijital imzalaması.

Uzaktan Müşteri Edinimi sürecini hızlandıran en önemli bileşenlerden birisi de yasal dijital imza ile yapılan kimlik doğrulama işlemidir.

Yönetmelikte uzaktan kimlik tespiti için kişinin açık rızasının elektronik ortamda kayıt altına alınması, kişinin kimlik belgesinin yakın alan iletişim (Near Field Communication-NFC) teknolojisi ile doğrulanması, kişinin görüşmeyi kendi isteği ile yaptığının doğrulanması ve banka tarafından gönderilen SMS'in OTP (One-Time Password) ile doğrulanması süreçleri yer almaktadır (Fintech İstanbul, 2021).

Finansal teknolojilerin bankacılıkta kullanılmasıyla birlikte geleneksel müşteri kabul süreçlerinin yanında uzaktan müşteri edinimi süreçlerinin de denetim kapsamına alınması ihtiyacı doğmuştur. Şube denetimlerinde örneklem yöntemi ile personel tarafından kimlik kontrolünün nasıl yapıldığı, üçüncü kişi işlemlerinde vekaletname bulunup bulunmadığı, yetkilerin yanı sıra yapılan işlemde talimatname olup olmadığı veya dekonta imza alınıp alınmadığı, banka sisteminde işlem yapan kişi ile gerçekte yapan kişi arasında fark olup olmadığı kontrol noktaları arasında bulunmaktadır.

Uzaktan müşteri edinimi süreçleriyle birlikte geleneksel müşteri kazanımından oluşabilecek operasyonel riskler en aza indirilmiştir. Uzaktan müşteri edinimi süreçlerindeki BT sistemlerinin doğru çalışıp çalışmadığı, elektronik ortamda yapılan görüşmede personelin sistemde belirtilen şekilde süreçleri ilerletip ilerletmediği örneklem yöntemi ile denetlenebilir. Ayrıca Bankanın bu hizmeti dış hizmet/destek hizmeti şeklinde alması halinde BDDK'nın "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" ve "Bankaların Destek Hizmeti

Almalarına İlişkin Yönetmelik" düzenlemeleri kapsamında risklerin bulunup bulunmadığı kontrol edilebilir.

2.2.2. Risk Yönetimi Faaliyetlerinin Denetimi

Bankanın risk yönetimi faaliyetleri iki şekilde ele alınabilir. Birincisi uyum birimi kapsamında suç gelirlerinin aklanması ve terörün finansmanının önlenmesine yönelik risklerin yönetilmesiyle ilgili faaliyetler; ikincisi ise Basel kriterlerine göre market riski, kredi riski gibi risklerin yönetilmesine yönelik faaliyetlerdir.

i. Uyum riski

Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelik'in 11. Maddesinde *"Yükümlüler, kurum politikası kapsamında, işletme büyüklüklerini, iş hacimlerini ve gerçekleştirdikleri işlemlerin niteliğini gözeterek risk yönetim politikası oluştururlar"* belirtilmiştir (Resmi Gazete, 2021). Bankalar da bu amaca yönelik risk yönetim politikasını oluşturarak riskleri yönetmektedir. Bankaların risk yönetim faaliyeti kapsamı;

- Riskli müşteri, işlem, hizmet veya ürünlerin tanımlanması, izlenmesi ve şüpheli olması durumunda gerekli yerlere bildiriminin yapılması,
- Risk tanımlama, sınıflandırma ve değerlendirme süreçlerinin değişen koşullara göre periyodik olarak değerlendirilmesi,
- Risk izleme ve değerlendirme sonuçlarının Banka Yönetim Kuruluna raporlanması,

faaliyetlerinden oluşur.

Bankalar düşük riskli müşteriler, yüksek riskli müşteriler ve yüksek riskli ürün, işlem ve hizmetler olmak üzere Banka müşteri, hizmet ve ürünleri risklilik derecelerine göre sınıflandırarak riskleri izler. Bu sınıflandırma yapılırken;

- FATF tarafından listeye alınan, kıyı bankacılığı yapılan, vergi cenneti olan, suç oranının yüksek ve yolsuzluğun yaygın olduğu ülkelerdeki müşteri ve işlemler,
- Yüksek tutardaki nakit, elektronik fon transferi işlemleri, muhabir bankacılık işlemleri, kiralık kasalar gibi hizmet ve ürünler

dikkate alınmaktadır.

ii. Diğer riskler

Bankalar kredi riski, piyasa riski, likidite riski, operasyonel risk, karşı taraf kredi riski, faiz oranı riski, artık risk, yoğunlaşma riski, ülke riski, itibar riski, deprem riski, iklim riski gibi uyum riski dışındaki risklerini risk yönetimi birimi tarafından yönetmektedir. Bu risklerin yönetilememesi durumunda mevzuata uyulmaması ve düzenleyici kurumlar tarafından ceza verilmesi sebebiyle bu riskler uyum riski ile de bağlantılıdır.

Banka iç denetim birimi uyum birimi ve risk yönetimi birimi tarafından gerçekleştirilen faaliyetlerin denetiminde; uyum programının ve senaryoların etkinliğini, birimin yaptığı risklilik sınıflandırmasını, risklilik sınıflandırılması ve senaryolara göre sistemin doğru çalışıp çalışmadığı, bu sınıflandırmaya göre izleme faaliyetlerinin yapılıp yapılmadığı, yasal mercilerce belirlenmiş rasyoların aşılıp aşılmadığı, iyi uygulama rehberlerine göre senaryoların ve modellerin belirlenip belirlenmediği, duyarlılık analizleri, içsel senaryo analizleri, stres testleri gibi uygulamalar ile risklerin izlenip sonuçlarına göre aksiyon alınıp alınmadığı kontrol noktaları arasında bulunmaktadır.

2.2.3. İzleme ve Kontrol Faaliyetlerinin Denetimi

Banka, müşterilerin işlemlerinin niteliğine göre izleme ve kontrol faaliyetlerini uyum birimi vasıtasıyla yürütmektedir. Bu faaliyetlerin amacı bankanın uyum riskini yönetmesi ve faaliyetlerinin çeşitli mevzuatlara uygun bir şekilde yapılıp yapılmadığının sürekli kontrol edilmesidir.

Bu kapsamda faaliyetlerin kapsamı; yüksek riskli müşteri ve işlemleri, riskli ülke veya bölgelerde gerçekleştirilen işlemler, olağandışı hareketler veya karmaşık işlemler, kimlik tespiti yapılması gereken tutarlardaki işlemler, gerçekleştirilen işlemlerin müşteri risk profiliyle uyumlu olup olmadığının kontrolü ve izleme faaliyetleridir (TBB-MASAK Çalışma Grubu, 2005: 87). İzleme ve kontrol faaliyetleri süreçlerinin etkinliği, faaliyetlerin gelişen teknolojilerle veya yeni ürünlerle yapılan işlemleri kapsayıp kapsamadığı, bu işlemler nedeniyle suistimale açık alanların değerlendirilerek kontrol faaliyetlerinin güncellenip güncellenmediği, izleme ve

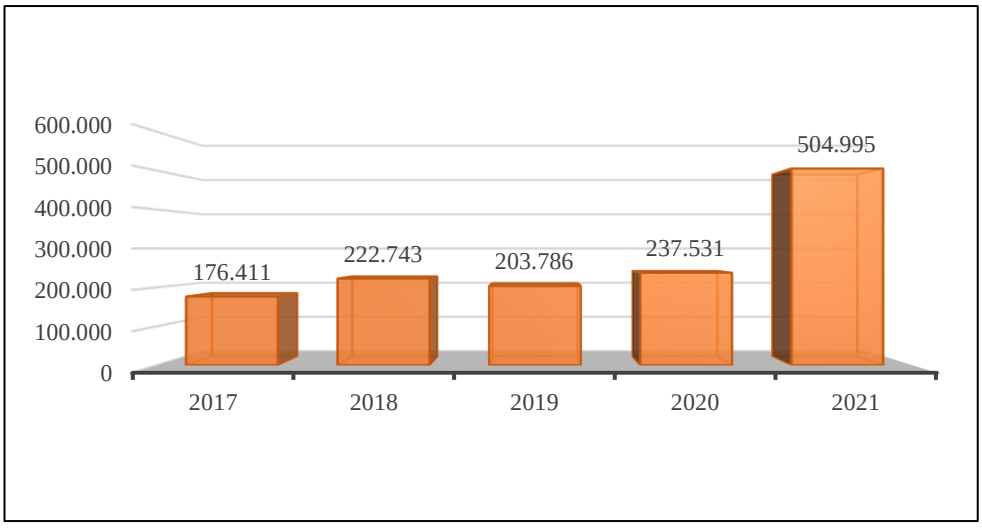
kontrol faaliyeti senaryolarının periyodik olarak değerlendirilip değerlendirilmediği banka iç denetim birimi tarafından kontrol noktası olarak değerlendirilebilir.

2.2.4. Şüpheli İşlem Bildirimleri Denetimi

Şüpheli işlem, Bankada yapılan işleme konu malvarlığının yasa dışı yollar ile elde edildiğine ya da bu amaçlarla kullanıldığına dair herhangi bir bilgi ya da şüpheli hususun bulunması durumudur. Şüpheli işlem bildirimi ile ilgili husus konusunda yetkili otoritelerin uyarılması ve bu işlemlerin yetkili otoritelerce de izlenmesi amaçlanmaktadır.

Banka şube veya genel müdürlük birimi personeli MASAK tarafından belirlenen şüpheli işlem tiplerine göre şüpheli işlem bildirimi yapabilir. İlgili personel böyle bir durumla karşılaştığında kimlik tespiti yaptıktan sonra Banka sisteminden şüpheli işlem tipini seçer, sayılı işlem tiplerinde yok ise neden şüphelendiğini belirtir, işlem şeklini ve tutarı seçerek uyum görevlisine raporlar. Bu bildirimler uyum görevlisi tarafından uygun görüldükten sonra MASAK'a iletilir. Uyum görevlisi MASAK'a bildirilmeyecek işlemler için görüşünün gerekçesini yazarak görüşü muhafaza eder. Şüpheli işlemler en geç on iş günü içerisinde MASAK'a bildirilmek zorundadır. Aksi durumda bankaya cezai yaptırım uygulanabilir.

Grafik 2.1 :Şüpheli İşlem Bildirimleri Yıllara Göre Dağılımı (2017-2021)



Kaynak: MASAK 2021: 15

Türkiye'de her yıl yakın seyreden işlem bildirimlerinin 2021 yılında dikkat çekici şekilde arttığı Grafik 2.1'de görülmektedir. Bu durumun nedeni son yıllarda gerçekleştirilen uyum denetimlerinin artması gösterilebilir (MASAK, 2021: 14).

Bankaya yasal otoritelerce yaptırım uygulanmaması için iç denetim birimi tarafından yapılacak denetimler önem arz etmektedir. Bu denetimlerde şüpheli işlem bildirimi sürecinin etkinliği, uyum görevlisine yapılan bildirimlerin yasal süreler içinde MASAK'a bildirilip bildirilmediği, bildirilmeyen işlemlerin mahiyeti örneklem yöntemi ile seçilip incelenebilir.

2.2.5. Oluşturulan Mevzuatın ve Yeni Ürünlerin Uygunluğunun Denetimi

Bankalar kendi faaliyetlerini ilgilendiren yasal otoritelerce çıkarılmış her türlü mevzuat değişikliğini takip etmek zorundadır. Bu sebeple Banka bünyesinde mevzuatı takip eden, değerlendiren, mevzuat değişikliklerini ilgili birimler ile paylaşıp koordinasyonu sağlayan, yeni çıkarılan ürünlerin mevzuata uygunluğu hakkında görüş veren bir birim bulunmaktadır.

Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliğin 18. Maddesinde "*Yeni ürün ve işlemler ile gerçekleştirilmesi planlanan faaliyetler için yönetim kurulundan onay alınmadan önce ikinci fıkra uyarınca görevlendirilen birimden görüş alınır*" belirtilmiştir (Resmi Gazete, 2014).

Bankalar yeni çıkaracakları ürün ve hizmetler için maruz kalacakları muhtemel riskleri belirlemeli ve değerlendirmelidir (BDDK, 2016: 19). Bankalar yeni ürün ile ilgili ilgili birimlerin görüşünün alındığı bir süreç oluşturmalı, muhtemel riskleri belirlemeli, mevcut risk iştahı ve kapasitesinde yaratacağı değişikliği değerlendirmeli, kontrol ve risk yönetim süreçlerini belirlemeli, kontrol sonrası oluşacak artık riski değerlendirmeli, bu faaliyetlerde kullanılacak prosedür ve ölçüm yöntemlerini belirlemeli ve yeni ürünü müşterilere sunmadan önce ürün ile ilgili sağlam bir teknolojik altyapı kurmalıdır (BDDK, 2016: 19-21).

Banka iç denetim faaliyeti kapsamında; yeni ürün sürecinin etkinliği, yeni ürün oluşturulurken ilgili birimlerinin görüşünün alınıp alınmadığı, bilgi teknolojileriyle ilgili sağlam bir altyapın oluşturulup oluşturulmadığı, yeni ürünün suç gelirlerini

aklama ve terörün finansmanı mevzuatlarınca uygun olup olmadığı, mevzuatı izleme ve değerlendirme süreçlerinin etkin olup olmadığı, ilgili birimlerce koordinasyonun sağlıklı yapılıp yapılmadığı, mevzuat değişikliklerine zamanında aksiyon alınıp alınmadığı kontrol noktası olarak değerlendirilebilir.

2.2.6. Eğitim Faaliyetlerinin Denetimi

Eğitim ile ilgili hususlar MASAK'ın Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelik'in altıncı bölümünde eğitim başlığı altında düzenlenmiştir.

Yönetmeliğe göre banka SGA/TF mevzuatı kapsamında eğitim politikası hazırlamak ve personellerini eğitmek ile yükümlüdür. Eğitimdeki amaç ilgili mevzuatlara uyumun sağlanması, personelin sorumluluk bilincinin artırılarak kurum kültürü oluşturulması ve bilgilerin güncel tutulmasıdır. Eğitimlerin kapsamı terimlerin kavramı, örnek olaylar, ulusal ve uluslararası mevzuat ve risk alanlarıdır. Banka eğitim ile ilgili istatistikleri her yıl belirli tarihlerde uyum görevlisi vasıtasıyla MASAK'a bildirir (TBB-MASAK Çalışma Grubu, 2005: 94).

Banka iç denetim faaliyeti kapsamında; eğitimde hangi hedef kitle personel grubunun seçildiği, yeni başlayan personele eğitim verilip verilmediği, eğitim programının mevzuat ile uyumlu olup olmadığı, eğitimin alanında uzman kişilerce verilip verilmediği, eğitim ile iliği istatistiki bilgilerin MASAK'a zamanında bildirilip bildirilmediği kontrol noktası olarak değerlendirilebilir.

2.2.7. KVKK Denetimi

Bankacılık sektörünü etkileyen son gelişmelerden biri de kişisel verilerin korunması konusudur. Avrupa Birliği'nde 24 Mayıs 2016 tarihinde yürürlüğe giren Genel Kişisel Veri Koruma Tüzüğü (General Data Protection Regulation-GDPR) ile birlikte Türkiye'de 6698 Sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016'da 29677 tarihli Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

Kişisel Verilerin Korunması Kanununun 12. madde 3. Fıkrasında *"Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır."* belirtilmiştir (KVKK, 2016). Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında

Yönetmelik ile birlikte müşteri sırrı, banka sırrı, kalıcı veri saklayıcısı, kimliksizleştirme, toplulaştırma gibi bazı kavramların tanımı yapılmıştır.

Bankalar kişisel verilerin korunması ile ilgili veri işleme, saklama ve imha süreçlerini oluşturmalı, politikalarını belirlemeli, tüm faaliyetlerini kanuna uyumlu hale getirmeli, bünyesinde KVKK irtibat kişisi belirlemeli, verisi işlenecek tüm müşterilerin açık rızasını almalı, personellerine de konu ile ilgili eğitimler vererek farkındalığı sağlamalıdır.

Banka iç denetim faaliyeti kapsamında; KVKK irtibat kişisinin olup olmadığı, KVKK süreçlerinin ve prosedürlerinin oluşturulup oluşturulmadığı ve bu süreçlerin etkin olup olmadığı, müşteri ve banka bilgilerinin korunması amacıyla teknolojik alt yapının etkin çalışıp çalışmadığı, müşterilerin KVKK ile ilgili şikayetlerini iletilebileceği bir kanalın bulunup bulunmadığı, bu şikayetler neticesinde herhangi bir veri sızıntısının olup olmadığı, verisi işlenen müşterilerin açık rıza belgelerinin olup olmadığı, bankanın siber saldırılarda müşteri ve banka sırrını saklamak için bilgi güvenliği süreçlerini etkin bir şekilde işletip işletmediği ve sistemde herhangi bir açık olup olmadığı kontrol noktası olarak değerlendirilebilir.

ÜÇÜNCÜ BÖLÜM
REGTECH EVRENİ VE BANKACLIKTA REGTECH

3. RegTech ve Bankacılık İlişkisi

Yoğun bir şekilde düzenleme ve denetim faaliyetlerinin gerçekleştirildiği bankacılık sektöründe uyum riski yönetimi için RegTech uygulamalarının kullanılması önemlidir. Çalışmanın bu bölümünde RegTech evreni, kullanılan teknolojiler ve RegTech'lerin hangi alanlarda çözüm geliştirdikleri anlatılmış, bankacılık sektöründeki teknolojik gelişmeler araştırılmış ve RegTech'lerin bankacılık sektörü ile ilişkisi incelenmiştir.

3.1. RegTech

RegTech ekosistemini oluşturan paydaşlar, RegTech çözümlerinin getirdiği faydalar ve uygulanmasındaki zorluklar ve sektörün geleceği aşağıdaki başlıklar altında incelenmiştir.

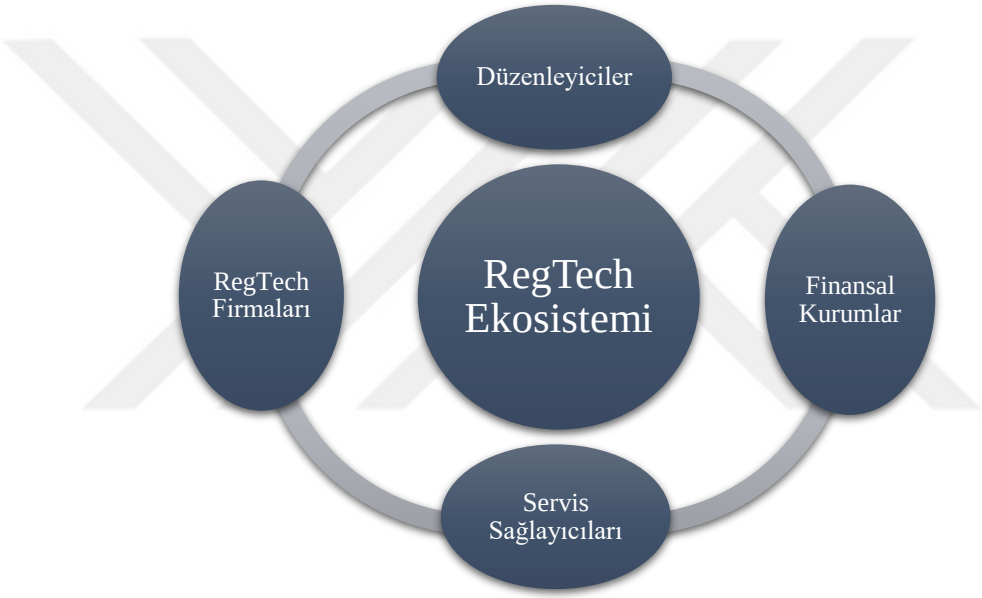
3.1.1. RegTech Ekosistemi

RegTech genellikle "Finansal Teknoloji"nin kısaltması olan FinTech (Financial Technology) ile karıştırılmaktadır. FinTech, tüketicilere daha iyi finansal hizmet sağlamak için teknoloji ve yazılımın kullanımına atıfta bulunurken, RegTech ise yasal otoritelerin çıkardığı düzenlemeler ile ilgili zorlukları karşılamak için gereken, giderek artan yoğun veri ortamını ele almak için yeni teknolojilerin kullanılmasına atıfta bulunur (EY 2019: 2). SupTech (Supervisory Technology) ise düzenleyici ve denetleyici otoritelerin faaliyetlerini gerçekleştirirken kullandıkları yeni teknolojileri ifade etmektedir (BCBS, 2018: 43). FinTech, bankaların teknoloji aracılığıyla müşterilerle bağlantı kurmasına yardımcı olduğu gibi, RegTech de bankaların teknoloji aracılığıyla mevzuat gerekliliklerini karşılamalarına ve SupTech de yasal otoritelerin bankaların mevzuat gerekliliklerini karşılayıp karşılamadıklarını denetlemelerine yardımcı olur.

RegTech bazı kaynaklarda FinTech'in alt kümesi olarak tanımlansa da (LexisNexis, 2022; FCA, 2016: 3) birbirinden farklı fenomenlerdir. FinTech en basit

tanımı ile teknolojinin finansal hizmetlerde kullanılmasıdır. RegTech ise herhangi bir finansal çözüm için gerekli olan uyum ve prosedürlerle ilgilenir. RegTech, finansal suçları önlemek için firmanın işlemlerini izleyip AML ve KYC gibi prosedürlere odaklanırken, Fintech ise işlemlerin son kullanıcılar ve çeşitli finansal kurumlar arasında gerçekleşmesini sağlar (Fineksus, t.y.(a)). Bir başka deyişle RegTech firmadan firmaya (Business to Business-B2B) FinTech ise firmadan tüketiciye (Business to Consumer-B2C) iş modeline sahiptir (Arner, v.d, 2016a: 85).

Şekil 3.1 : RegTech Ekosistemi

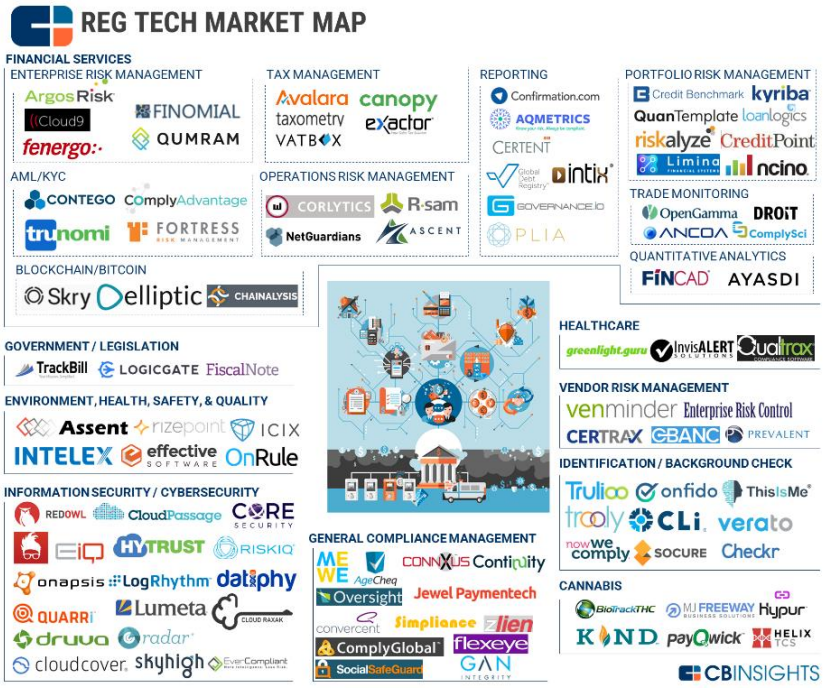


Kaynak: Rampton, 2023

RegTech ekosisteminde birbirleri ile ilişkili paydaşlar bulunmaktadır. Bu paydaşlar Şekil 3.1'deki şemada gösterilmiştir. Bu ekosistemde düzenleyiciler sektörün kurallarını belirler, finansal kurumlar müşterilerine çeşitli hizmet ve ürün sağlar, servis sağlayıcıları bu faaliyetlerin müşterilere ulaşmasını sağlarken RegTech firmaları da bu kurumların çeşitli kurallara uymalarına yardımcı olur.

Ekosistemin başarılı bir şekilde devam edebilmesi için düzenleyiciler ortak bir diyalog ortamı oluşturarak sektör görüşlerini toplamalı ve yeniliğe teşvik etmelidir. RegTech firmaları finansal kurumların ve düzenleyicilerin ihtiyaçlarını karşılayacak çözümler geliştirirken finansal kurumlar da bu çözümleri benimsemelidir (Rampton, 2023).

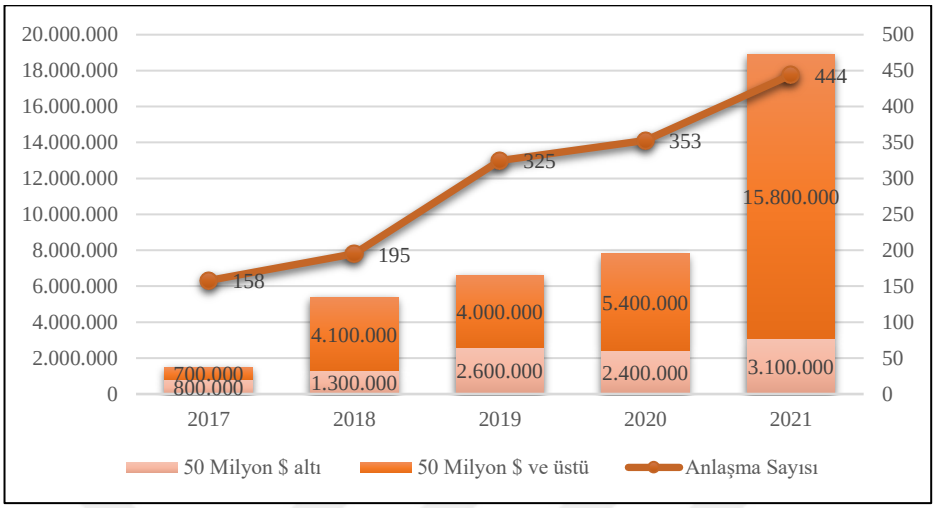
Şekil 3.2 : RegTech Sektör Haritası



Kaynak: Cbinsights, 2017

Deloitte'un 2023 RegTech Evreni çalışmasına göre yasal raporlama alanında 83, risk yönetimi alanında 68, kimlik yönetimi ve kontrolü alanında 93, uyum alanında 199 ve işlem izleme alanında 38 olmak üzere toplamda 485 RegTech firması bulunmaktadır (Deloitte, t.y.(b)). Bu firmaların arasında Türkiye'de işlem izleme alanında "Fineksus", risk yönetimi alanında "Nerodata" ve kimlik yönetimi ve kontrolü alanında "Sanction Scanner" isimli firmalar bulunmaktadır. Tüm RegTech sektörüne baktığımızda Türkiye'de 3 firmanın bulunması Türkiye'deki RegTech sektörünün yolun başında olduğunun göstergesidir.

Grafik 3.1 :Yıllara göre RegTech yatırımları



Kaynak: Fintech Global, 2022

Grafik 3.1'de 2017-2021 yılları arasında yapılan RegTech anlaşmaları ve yatırım tutarları gösterilmiştir. 2021 yılında RegTech firmaları 444 anlaşmada 18,9 milyar $ toplayarak bir önceki yıla göre 2 katından daha fazla yatırım almıştır. Bu artışın sebebi Covid-19 önlemleri kapsamında sosyal mesafe önlemleri ve esnek çalışma düzeni getirilmesi dolayısıyla finansal kurumların çevrimiçi riskleri yönetmek ve uzaktan personelin davranışlarını izlemek için dijital çözüm arayışına girmesinden kaynaklandığı belirtilmiştir (FinTech Global, 2022). Pandeminin dijitalleşmeyi hızlandırmasıyla da finansal kurumların siber güvenlik alanına daha fazla yatırım yapmasına yol açmıştır.

3.1.2. RegTech Fayda ve Zorlukları

Firmaların mali suçlarla mücadele etmek ve gelişen düzenlemelere uyum sağlamak için teknolojik çözümler araması gerekir (Von Solms, 2021: 152). Bu nedenle, hizmet sağlayıcıların yasal uyumluluk yükümlülüklerini yerine getirmek ve finansal sistemi zarar görmekten korumak için RegTech'in kendilerine nasıl yardımcı olabileceğini anlamaları önemlidir. RegTech'in firmalar için faydaları üç bölümde özetlenebilir:

i. *Tasarruf:* Mevzuata uyum faaliyetleri firmalar için maliyetlidir. Bu nedenle para tasarrufu, firmaların RegTech çözümlerini benimsemesinin ana nedenlerinden biridir. Ayrıca mevzuata uyum zaman, kaynak ve çok sayıda iş

gücü gerektirir. RegTech'in mevcut yasal uyumluluk süreçlerini iyileştirmesi, firmaların tasarruf etmesine yardımcı olabilecek basit bir yoldur (Nguyen, 2017: 33). RegTech, doğru bir şekilde uygulandığı takdirde firmalara işe alım aşamasından bir müşterinin sürekli olarak izlenmesine kadar veri kalitesine daha tutarlı bir yaklaşımla yardımcı olabilir (Linda ve Bailey, 2022). Düzenleyici veriler RegTech çözümleri uygulanarak çok daha verimli bir şekilde toplanıp analiz edilebilir. Bu da iş gücünden, zamandan ve paradan tasarruf sağlamak anlamına gelmektedir.

ii. *Müşteri Deneyimini İyileştirmek*: Daha iyi bir müşteri deneyimi için RegTech bir katalizör görevi görerek firmanın markasının doğru bir şekilde tanıtılmasını sağlar (Barrere, 2020). Ayrıca risk değerlendirmesi, entegrasyon araçları, yapay zekâ gibi RegTech teknolojileri, müşteri bilgilerinin daha niteliksel olarak analiz edilmesini ve müşteri davranışı hakkında zengin verilere erişimi sağlayarak müşteri deneyiminin geliştirilmesine katkıda bulunur (Vivek, v.d. 2020: 10). Gizlilik de önemli olduğu için e-posta yerine dijital olarak güvenli bir platform aracılığıyla bilgi sağlamak da müşteri deneyimine katkıda bulunur (Linda ve Bailey, 2022).

iii. *Riskin Azaltılması:* RegTech çözümleri, firmaların kendilerini yasal ihlal riskinden korumalarına yardımcı olabilir. Bunlar genellikle Bulut Bilgi İşlem, Uygulama Programı Arayüzü (API), Büyük Veri ve Analitik ile Ses ve Metin Tanıma gibi temel teknolojilere dayanır. Bugün birçok RegTech firması, yasal uyumluluk ve düzenleyici konular hakkında gerçek zamanlı uyarılar sağlayarak risk yöneticilerinin ilgili düzenleyici değişikliklerden haberdar olmalarına yardımcı olmaya kendini adamıştır (Nguyen, 2017: 33). Ayrıca, RegTech Covid-19 salgınıyla artışa geçen siber suç olaylarına, para hırsızlığına ve tıbbi dolandırıcılıklara karşı mücadelede önemli bir unsur olmuştur (Salami, 2020: 410). RegTech çözümleri, finansal kurumlara daha fazla sayıda müşteriyi firma baskısı ve pandeminin etkileri nedeniyle artan uyumluluk yükünün yönetilmesine yardımcı olmuştur (Comply Advantage, 2022). RegTech çözümleri ile riskleri ve tehditleri tespit etmek ve bu riskleri yönetmekten sorumlu olanları uyarmak için gerçek zamanlı veriler

bilgisayarlarla izlenerek risk yönetimi süreçleri otomatikleştirilmektedir (Singh ve Lin, 2020: 474).

RegTech'in faydalarının yanında uygulamada zorluklar da bulunmaktadır. Bu zorluklar üç bölümde özetlenebilir:

i. *Standart Olmayan Düzenlemeler:* 2008 küresel mali krizinden bu yana düzenlemeler standartlaştırılmaya çalışılmıştır. Fakat yine de ulusal ve uluslararası düzenlemeler hala gelişmekte ve karmaşık olduğu için bu önemli bir sorun olarak görülmektedir (EBA, 2021c: 31). Farklı ülkelerdeki düzenleyiciler arasındaki farklılıklara ek olarak, aynı yetki alanındaki düzenleyiciler arasında da çatışmalar ortaya çıkabilir (Saucier, 2022). Dünya çapında müşterilere hizmet veren firmalar için zorluk, bir ülkeden diğerine farklı uyumluluk gereksinimlerini yönetmektir (Aktaş ve Roland, 2021: 87). RegTech bu zorluklarının üstesinden gelmeye yardımcı olabilir fakat doğru yazılımı seçmek önemlidir.
ii. *Siber Güvenlik:* Firmaların, güvenli önlemler seçerek olası bir siber saldırıdan kaçınmak için ekstra adımlar atması gerekmektedir. Bu nedenle RegTech firmaları, siber güvenlik uygulamalarının hassas firma verilerini koruduğundan emin olmalıdır. Tüketici tabanlarının güvenini kazanmak ve sürdürmek için bu uygulamalardaki değişikliklere sürekli ayak uydurmaları ve güncel yazılımları kullanmaları önemlidir.
iii. *Eski sistemler:* Firmalar, birçok avantajına rağmen RegTech çözümlerini benimsememektedir. Bunun nedeni ise firmaların genellikle yeni teknolojilerle entegre olmayan veya birçok değişiklik gerektiren eski sistemlerdir (Cowburn ve Barnet, 2019). Bu eski sistemleri değiştirmek için firmaların yatırım yapması ve bu yatırımın tamamlanmasını beklemesi gerekir. Bu nedenle yeni sistemlere geçiş ve RegTech çözümlerini benimsemeleri gecikmektedir (Arner, v.d., 2015: 33).

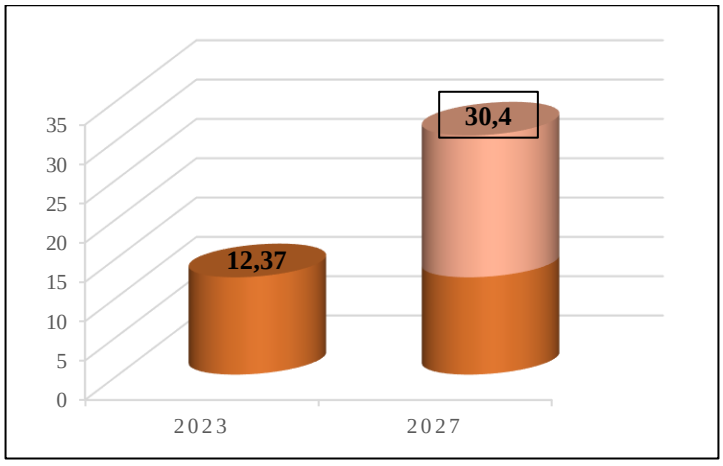
3.1.3. RegTech Sektörünün Geleceği

Finansal kurumlar artan uyumluluk maliyetleri ve yeni düzenlemeler getirecek yeni hizmetler ve ürünler geliştirdikçe RegTech gelişmeye devam edecektir. Ayrıca

her sektörde ve özellikle finansal hizmetlerde gelecekte kolaylaştırılmış uyum süreçleri daha fazla otomasyon ve standardizasyon gerektirecektir (Tyagi, 2021). RegTech'in arka ofis işlevinde halihazırda oynadığı role ek olarak uzmanlığı ve bilgisi ön büro operasyonlarını ve stratejilerini etkili bir şekilde kolaylaştırabilecektir (Mulder, 2019).

Kurumlar artan düzenleyici karmaşıklık ve incelemeyle karşı karşıya kaldıkça finans sektöründe RegTech çözümlerinin daha fazla benimsenmesi beklenebilir. Uyum süreçlerini desteklemek için daha gelişmiş makine öğrenimi ve yapay zekâ yetenekleriyle RegTech çözümleri giderek daha fazla otomatik hale gelecektir. Finansal kurumlar ve RegTech sağlayıcıları, belirli yasal gereklilikleri karşılayan özelleştirilmiş çözümler geliştirmek için daha yakın iş birliği yapacaktır. RegTech çözümleri, veri gizliliğini, güvenliğini ve şeffaflığını geliştirmek için blok zinciri gibi diğer teknolojilerle de birleşerek faaliyet alanlarını genişleteceklerdir. RegTech çözümleri daha yaygın hale geldikçe sektörün uyum konusunda inceleme ve gözetiminin arttığı da görülebilir. Genel olarak RegTech finansal kurumlar için mevzuata uygunluk süreçlerini dönüştürme, verimliliği, doğruluğu ve şeffaflığı artırma, maliyetleri düşürme ve riski azaltma potansiyeline sahip olduğu için finansal kurumlar tarafından kullanılmasıyla yaygınlaşacaktır.

Grafik 3.2 : RegTech Sektörü Büyüme Tahmini (Milyar $)



Kaynak: Researchandmarkets, 2023

Grafik 3.2'de RegTech marketinin 2027 yılında tahmin edilen market büyüklüğü görülmektedir. Researchandmarkets'in 2023 yılı "RegTech Küresel Pazar

Raporu"nda küresel RegTech pazarının %24,5'lik yıllık bileşik büyüme oranıyla 2022'de 9,93 milyar $'dan 2023'te 12,37 milyar $'a yükseldiği, Rusya-Ukrayna savaşının birden fazla ülkeye yönelik ekonomik yaptırımlara, emtia fiyatlarında artışa ve tedarik zinciri kesintilerine yol açarak mal ve hizmetlerde enflasyona neden olduğu ve COVID-19 salgınının ekonomik etkilerinden kurtulmanın önüne geçtiği, bu savaşın dünya çapında birçok pazarı etkilediği ve RegTech pazarının da bundan etkilendiği, RegTech pazarının 2027'de %25,2'lik bir yıllık bileşik büyüme oranıyla 30,4 milyar $'a çıkması beklendiği belirtilmiştir (Researchandmarkets, 2023).

3.2. RegTech Altyapısı

RegTech yazılımlarının geliştirilmesinde çeşit teknolojiler kullanılmaktadır. Bu teknolojilere aşağıda yer verilmiştir.

3.2.1. Yapay Zekâ

Yapay zekâ (Artificial Intelligence-AI), "akıllı" makineler inşa etmeyi amaçlayan, insan zekâsı ve yetenekleri gerektiren görevleri yerine getirebilen ve bilgisayar sistemlerinin geliştirilmesini sağlayan bilgisayar bilimidir (BCBS, 2018: 42).

Yapay zekâ insan kapasitesini aşacak düzeyde büyük verileri düşük marjinal maliyet ile işler ve insan gözünden kaçabilecek ilişkileri ortaya çıkarmaktadır (Wall, 2018: 55). Yapay zekanın uygulama alanlarına bakıldığında; sesleri tanıma, görüntü ve lisan işleme, muhakeme yapma özelliklerinin kullanıldığı görülmektedir. Günlük hayatta sesli asistanlar, navigasyon, sağlık hizmetleri, e-ticaret, sosyal medya, otonom sürüş uygulamaları gibi alanlarda kullanılmaktadır.

Finans sektöründe ise yapay zeka bankalarda kredi tahsis süreçlerinde, kredi riskinin azaltılmasında, sermaye piyasalarında hisse alım satım işlemlerinde, mevzuata uyum kapsamında yapılan denetimlerde fayda sağlamaktadır (WEF, 2018: 18). RegTech uygulamaları üzerinde benzer özellikteki müşteri işlemlerini gruplandırma, anormallikleri tespit etme, analistler tarafından yapılan hatalı değerlendirmeleri öğrenerek erken uyarı oluşturma, şüpheli müşteri davranışlarını tespit etme gibi faaliyetler ile AML konularında faydalı olmaktadır (Wright, 2019).

3.2.2. API

API İngilizce'de Application Program Interface'nin kısaltması olarak kullanılan ve "Uygulama Programı Arayüzü" anlamına gelen, yazılım programlarının birbirleriyle etkileşime girmesini sağlayan bir dizi araç, protokol ve kuraldır (BCBS 2018: 42). API'ler, uygulamalar arasındaki iletişimi sağlar ve bu etkileşimin nasıl yürütülmesi gerektiğini belirler. Çeşitli yazılım programlarının mimari farklılıklarına rağmen bilgilerin doğru bir şekilde aktarılabilmesini sağlar. Diğer bir deyişle, API'ler veri ve hizmet talep edenleri ve sağlayıcıları birbirine bağlayan haberciler olarak görülebilir (Johl, 2022).

API'lerin temel özelliklerinden biri, geliştiricilerin önceden var olan kodlar ve programlar üzerine geliştirmelerine izin vermesidir. Geliştiriciler kodu sıfırdan yazmak yerine, uygulamalarına belirli verileri veya işlevleri uygulamak için mevcut API'leri kolayca kullanabilir (Johl, 2022).

API'ler ayrıca Açık Bankacılığın yapı taşı olarak görülmektedir. Finansal teknolojilerin gelişmesiyle birlikte bankalar API altyapılarını geliştirerek birbirlerinin kullanımına açmaya ve müşterilerine yeni ürünler sunmaya başlamıştır.

Verilerin toplanması, yönetimi ve dağıtımını teşvik eden API teknolojisi RegTech girişimlerinde özellikle yararlı olabilir.

3.2.3. Büyük Veri

Büyük veri (Big Data) terimi, genel olarak dijital araçların ve bilgi sistemlerinin artan kullanımıyla üretilen büyük hacimli yapılandırılmış ve yapılandırılmamış verileri ifade etmektedir (BCBS 2018: 42). Büyük veri analitiği ise bu büyük ve karmaşık veri setlerinin yararlı bilgiler elde etmek amacıyla analizi için kullanılan çeşitli yöntemlerdir.

Büyük veri, 5V olarak adlandıran kavramları içermektedir. Bunlar; hacim (Volume), hız (Velocity), çeşitlilik (Variety), gerçeklik (Veracity) ve değer (Value) kavramlarıdır. Hacim, üretilen verinin büyüklüğünü; hız, verinin yayılma hızını; çeşitlilik, sayısal, sözel, görsel vb. veri türlerini; gerçeklik, verinin güvenilirliğini veya doğruluğunu; değer ise büyük verinin kullanılması sonucu yaratılan değeri ifade etmektedir (Aktan, 2018: 4-6).

Devasa boyuttaki veri kümelerinden istenilen bilgiye ulaşılması için veri madenciliği diye adlandırılan teknikler geliştirilmiştir. Verideki modelleri keşfetme süreci olarak da tanımlanan veri madenciliğinde, büyük veri içerisindeki potansiyel ve gerekli bilgiler çıkarılıp kullanıcıya sunularak çeşitli alanlarda kullanılır (Witten ve Frank, 2005: xxiii).

Bankacılık alanında veri madenciliği, pazarlama faaliyetlerinde, müşteri profili analiz edilmesinde, kredi tahsis süreçlerinde, dolandırıcılık faaliyetlerinin tespit edilmesinde kullanılmaktadır.

Büyük verinin RegTech ile ilişkisine bakıldığında, veri madenciliği ve büyük verinin RegTech çözümlerini desteklediği düşünülmektedir (Deloitte, 2018b: 4). RegTech yazılımlarının uyum riski ile ilgili çözümlerini sunabilmesi için doğru, güvenilir ve yeterli veriye ihtiyacı vardır. Veri madenciliği ile kompleks veri kümesinden ilgili ve anlamlı veriyi elde ederek çözüm üretebilmektedir.

3.2.4. Blok zinciri

Dağıtık Defter Teknolojisi (distributed ledger technology-DLT), birden fazla veri deposunda bilgilerin kaydedilmesini, paylaşılmasını ve senkronize edilmesini sağlayan, dağıtık defterinin ağ katılımcıları tarafından yaygın olarak paylaşıldığı ve sürekli güncellenen veritabanına sahip olan bir teknolojidir. Blok zinciri (Blockchain) ise DLT'nin bir uygulamasıdır (Natarajan, Krause ve Gradstein, 2017: 1).

2008 yılında bir kişi Satoshi Nakamoto takma adıyla katılımcıların finansal aracılara güvenmeden doğrudan çevrimiçi ödeme yapmalarını sağlayan eşler arası bir dijital nakit sistemi olan Bitcoin'i ve onun altında yatan blok zinciri teknolojisini tanıtan teknik bir inceleme kaleme almıştır (Nakamoto, 2008). İlgili yazı ile ademi merkeziyetçilik sağlanmış ve çifte harcama sorunu yani aynı varlığın birçok tarafa gönderilme olasılığını ortadan kalkmıştır.

Blok zinciri teknolojisinde işlem verileri "blok" adı verilen gruplara ayrılır. Her yeni blok işlem kayıtlarının veritabanı olan dijital bir "zincir" aracılığıyla öncekilerle bağlantılıdır. Her yeni giriş şifrelenir ve ağ katılımcıları tarafından ilgili defterlere kabul edilmeden önce doğrulanır. Yeni blok sadece tüm ağ tarafından doğrulandıktan sonra dağıtık deftere eklenir. Böylece güven ve şeffaflık sağlanmış olur.

Blok zinciri teknolojisi çeşitli potansiyel faydaları sayesinde RegTech firmaları tarafından kullanılmaktadır. Bunlardan biri AML ve KYC süreçleridir. Bankalar potansiyel müşterileri için kendi verilerini toplaması ve bu verileri düzenli olarak güncellemesi gerekmektedir. Bunun çözümü olarak blok zinciri teknolojisiyle tüm bankaların müşterilerinin tanımlanması ve işlemlerinin izlenebilmesi için evrensel bir dağıtık defter kullanılabilir. Bunun dışında blok zincirinin sağladığı şeffaflık sayesinde RegTech firmaları işlem izleme, kayıt tutma, fon yönetimi gibi faaliyetlerde bu teknolojiyi kullanmaktadır (Planet Compliance, t.y.).

3.2.5. Akıllı Sözleşmeler

Akıllı sözleşme (Smart Contrats), bir sözleşmenin performansını veya müzakeresini dijital olarak uygulamak, doğrulamak veya kolaylaştırmak için blok zinciri teknolojisini kullanan ve kendi kendine çalışan bir sözleşme olarak tanımlanabilir (Christidis ve Devetsikiotis, 2016: 2292). Blok zinciri teknolojisinin sergilediği güvenlikli ve merkezi olmayan sistem sayesinde, akıllı sözleşmeler, normal sözleşmelerde sergilendiği gibi üçüncü taraflara ihtiyaç duymadan sözleşme tarafları arasında işlem güvenilirliğini artırabilir.

Geleneksel sözleşmelerin bu dijital evrimi, firmalar, hükümetler ve diğer kullanıcılar için çeşitli avantajlar sağlayabilir. Akıllı sözleşmelerin mimari özellikleri, işlemlerin doğruluğunu, şeffaflığını ve güvenliğini artırmaktadır. Sözleşmenin yürütülmesi, resmi bir programlama diline, açıkça tanımlanmış şartlara ve dağıtılmış bir deftere dayanması sebebiyle insan müdahalesini ortadan kaldırmış, bu da ortak sözleşmelerde gözlemlenebilecek manuel hata ve yanlış anlama olasılığının düşük olmasını sağlamıştır (Nzuva, 2019: 71).

Akıllı sözleşmeler, geleneksel sözleşmelere göre uygun maliyetli bir alternatif olarak görülmektedir (Nzuva, 2019: 72). Ayrıca iş anlaşmalarının yürütülmesinde verimliliğin ve hızın artmasına da katkıda bulunmaktadır. Akıllı sözleşmelerin halen yasal bir zeminde olmamasına rağmen gelecekte finans sektöründe daha verimli, güvenilir ve hızlı süreçler için büyük bir potansiyele sahiptir.

Akıllı sözleşmelerin kullanımı RegTech çözümlerinin daha etkin olmasını sağlamaktadır. Bu sözleşmeler yasal zemine oturtulduğunda ve kullanımı

yaygınlaştığında RegTech yazılımları ile sözleşmelerin düzenlemelere uyumu daha hızlı ve güvenli bir şekilde yapılabilecektir. Banka veya firmanın yasal raporlama yaparken akıllı sözleşmelerin özellikleri sayesinde tutarsız veri göndermek imkansızdır ve her hata önceden engellenmektedir. Bu da veri toplama, inceleme, düzeltme ve raporlama faaliyetlerinde kullanılan eforun düşmesini ve maliyetin azalmasını sağlamaktadır (Regnology, 2022: 3-4).

3.2.6. Nesnelerin İnterneti

Nesnelerin İnterneti (Internet of Things-IoT), internet kullanımı yoluyla birbirine bağlı cihazlar kavramını ifade eder. Bu sistemde, "akıllı" cihazlar bir ağa ve/veya birbirine bağlanarak iletişim kurabilir ve veri paylaşabilir. Böylece, insan müdahalesine olan ihtiyaç azaltılmış olur (Figliola, 2020: 1).

Bir IoT ekosistemi, ortamlarından elde ettikleri verileri toplamak, göndermek ve bunlara göre hareket etmek için işlemciler, sensörler ve iletişim donanımı gibi gömülü sistemleri kullanan web özellikli akıllı cihazlardan oluşur. Bu cihazlar topladığı verileri analiz edilmek üzere başka bir bağlı cihaza aktararak paylaşır. Bazen bu cihazlar diğer ilgili cihazlarla iletişim kurar ve birbirlerinden aldıkları bilgilere göre hareket eder. Bu işlemler genelde insan müdahalesi olmadan yapılmaktadır fakat insanlar cihazların kurulması, talimat verilmesi, veriye erişilmesi gibi işlemler yapmak için cihazlar ile etkileşim kurabilmektedir (Gillis, 2022).

IoT teknolojisi, teknolojik araçların gelişmesiyle birlikte akıllı ev ve şehir sistemlerinde, tarım, taşımacılık, savunma gibi birçok sektörde kullanımı yaygınlaşmaktadır. Bankacılık sektörüne baktığımızda, kamera sistemleri, POS ve ATM cihazları gibi ekipmanlarda kullanılmakta, müşterilerin yaptıkları bankacılık işlemleri için dekont veya sözleşmelere imza atmak yerine mobil bankacılık üzerinden dijital imza atabilmekte, ATM üzerinden banka kartı olmadan mobil bankacılık üzerinden QR kod oluşturarak işlemlerini yapabilmektedir.

RegTech açısından bakıldığında, IoT teknolojisi kullanılan cihazların artmasıyla birlikte daha fazla verinin elde edilmesi sağlanacak ve bu verilerin analiz edilmesi ile daha etkin çözümler ortaya çıkacaktır.

3.2.7. Bulut Teknolojisi

Bulut teknolojisi (Cloud Technology), internet (Cloud) üzerinden bilgi işlem hizmetlerinin isteğe bağlı olarak sağlanmasını ifade eder. Bu hizmetler sunucuları, depolamayı, veri kümelerini, ağları, yazılımları ve hatta blok zinciri ve yapay zekâ uygulamalarını içerebilir (Microsoft Azure, t.y.).

Firmalar, kendi bilgi işlem altyapılarına veya veri merkezlerine sahip olmak yerine, bir bulut hizmeti sağlayıcısından uygulamalardan depolamaya kadar her şeye erişim kiralayabilir. Bulut bilişim hizmetlerini kullanmanın bir avantajı, firmaların kendi BT altyapılarına sahip olmanın ve bakımını yapmanın ön maliyet ve karmaşıklığından kaçınabilmeleri ve bunun yerine kullandıkları kadar kullandıklarında ödeme yapmalarıdır. Buna karşılık, bulut bilişim hizmetleri sağlayıcıları, aynı hizmetleri geniş bir müşteri yelpazesine sunarak önemli ölçek ekonomilerinden yararlanabilir (Ranger, 2022).

Bulut Bilişim sistemlerinin çeşitlerine bakıldığında üç tür bulut hizmeti vardır (Mell ve Grance, 2011: 2-3):

- Yazılım uygulama sağlayıcılarının müşterilerin hizmetlerini internet üzerinden, örneğin bir web tarayıcısı kullanarak kullanmalarına izin verdiği Hizmet Olarak Yazılım (Software as a Service-SaaS)
- Bulut sağlayıcılarının müşterilerin kendi uygulamalarını geliştirmek ve çalıştırmak için bulut altyapısını bir platform olarak kullanmalarına izin verdiği Hizmet Olarak Platform (Platform as a Service-PaaS)
- Bulut sağlayıcılarının müşterinin altyapısının ana bilgisayarı haline geldiği veya diğer bir deyişle bilgi işlem kaynaklarını kendilerine kiraladıkları Hizmet Olarak Altyapı (Infrastructure as a Service-IaaS).

RegTech ile bulut bilişim sistemleri ilişkisine bakıldığında RegTech, bir yazılım sistemi kurmak ve yasal düzenlemeler değiştiğinde güncellemek için acele etmek yerine firmalara sürekli güncellenen bulut tabanlı yazılım çözümleri sağlayabilir (Initium, t.y).

3.2.8. Robotik Süreç Otomasyonu

Robotik süreç otomasyonu (Robotic Process Automation-RPA), dijital sistemler ve yazılımlarla etkileşime giren insan eylemlerini taklit eden yazılım robotlarını oluşturmayı, devreye almayı ve yönetmeyi kolaylaştıran bir yazılım teknolojisidir (Uipath, t.y.). Bu teknoloji ile finans kurumları, insan muhakemesi gerektirmeyen sıkıcı manuel görevleri yazılım özellikli robotlarla değiştirerek verimliliği artırabilir ve önemli maliyet tasarrufları elde edebilir. Böylece insan hataları ve bunlara bağlı operasyonel riskler de azaltılmış olur. Robotlardan yararlanılarak yasal uyum ve risk yönetimi süreçleri daha doğru ve verimli yönetilebilir.

RPA'nın yapay zeka ile birleşimi ile akıllı süreç otomasyonu (Intelligent process automation-IPA) denilen kavram ortaya çıkmıştır. Bu otomasyonla birlikte önceden tanımlanmış görevlerin yürütülmesi, gelişmiş veri işleme ve karar verme işlemler yapılabilmektedir. Basit otomasyondan akıllı otomasyona geçiş, finansal kurumlar için önemli fırsatlar yaratabilir (EY, 2019).

Robotik süreçlerin kullanım alanlarına bakıldığında (Katara, 2018: 3-4);

- Yasal raporlamalar: Kısa sürede doğru raporlar hazırlamak için veri toplama ve konsolidasyonun otomatikleştirilmesinde kullanılabilir. Sorumlu personeller daha kritik görevlere odaklanabilir ve daha yüksek kaliteli raporlar çıkarabilirler.
- KYC/AML süreçleri: Müşteri kabulü süreçlerinin otomatikleştirilmesinde kullanılabilir. RPA, düzenleyici kurumlar gibi kaynaklardan ilgili verileri toplayabilir ve KYC kontrollerinde yer alan adımları uygulayabilir.
- Mali suç soruşturması: RPA, AML izleme sistemleri tarafından oluşturulan uyarıların incelenmesini otomatik hale getirebilir.
- Stres testi ve Model Doğrulama: RPA, yüksek hacimli, standartlaştırılmış iş akışlarının otomasyonu için kullanılabilir.

3.3. RegTech Çözümleri

Bankacılık sektörünün uyum riski konularında ihtiyaç duyduğu RegTech çözümleri aşağıdaki başlıklar altında incelenmiştir.

3.3.1. Uyum

Mevzuata uyum (General Compliance), kanunlar, genelgeler, tebliğler, politikalar ve tavsiye kararlar aracılığıyla öngörülen ihtiyati kuralların karşılanmasını ve ilgili tüm direktiflere uymak için atılan adımlardan oluşur. Bankalar her geçen gün artan bankacılık alanındaki düzenlemelerin yanı sıra içinde bulundukları diğer faaliyet alanlarındaki düzenlemeler konusunda da güncel kalmak zorundadır.

Değişen düzenlemelerle birlikte bankaların operasyonlarını değiştirmek için gereken süre de kritiktir. Çünkü bir düzenleme yürürlüğe konar konmaz günler içinde düzenlemeyi ihmal etme ihtimali bulunmaktadır. Bu sebeple bankaların mevzuata uyum faaliyetlerinde otomasyon sağlaması, hızlı tepki vererek düzenlemeye uyması ve bu faaliyetlerini de optimal maliyet ile yapması RegTech yazılımları ile gerçekleştirilebilmektedir (Solms, 2021: 196).

RegTech yazılımları kullanılarak basit görevlerin otomasyonunun yanında dinamik uyum süreçleri tasarlanabilir. Bu süreçlerde uyum düzeyi ve riskler gerçek zamanlı olarak izlenebilir ve operasyonel veriler bilgi sistemleri yardımıyla analiz edilebilir (Toronto Centre, 2017: 9). Böylelikle mevcut emek yoğun süreçler yerine otomasyon kullanılarak yeni düzenlemelere uyum sağlama ve esneklik artırılmış olacaktır.

3.3.2. Kimlik Yönetimi ve Kontrolü

Kimlik yönetimi ve kontrolü (Identify Verification) finansal düzenlemelerin ayrılmaz bir parçasıdır. Bankalar kendilerini mali, itibari ve hukuki zarar görme olasılığına karşı korumak için karşı taraf ile ilişki kurmadan önce müşterisini dikkatle incelemesi gerekmektedir. Bu incelemeyi de KYC prosedürlerine uygun olarak gerçekleştirmektedir. Bu süreç genelde müşterinin finansal faaliyetlerinin ve bunların risk faktörlerinin değerlendirilmesinin yanı sıra çeşitli kişisel belgelerin toplanmasını, doğrulanmasını ve analiz edilmesini içermektedir (Adl ve Haworth, 2018: 2). Bu süreçlerin uygulanması AML ve CFT prosedürlerinin gerçekleştirilmesi için gereklidir.

AML ve KYC süreçleri RegTech'e olan talepte itici bir güç haline gelmiştir. Bu prosedürlerin artan maliyetleri uyumu basitleştiren araçlara olan ihtiyacı

doğurmuştur (Arner, v.d., 2017: 9). RegTech yazılımları uyum maliyetlerini azaltmada ve mevcut süreçleri hızlandırmada yardımcı olabilir. Otomasyon sistemlerinin kullanılmasıyla hata oranı en aza indirilerek veri toplama ve analiz edilmesi kolaylaşır.

Uzaktan müşteri edinimi süreçleri, çağrı merkezi hizmetleri, video arama ile müşteri temsilcisi görüşmeleri gibi faaliyetlerin yaygınlaşmasıyla birlikte dijital kimlik doğrulaması için de RegTech yazılımlarının kullanılması bir banka için gerekli hale gelmiştir. Çeşitli müşteri bilgilerini içeren veri kümesini kullanan bir RegTech yazılımı, KYC prosedürlerini kullanarak bankanın yasal gereklilikleri yerine getirmesine yardımcı olur (Solms,2021: 196). Ayrıca taklit imzaların tespit edilmesi, telefon sesinden müşterinin kimliğinin tespit edilmesi, sahte kimlik kartı veya pasaport gibi kimlik dolandırıcılıklarını RegTech yazılımları ile önlemek mümkündür.

3.3.3. Risk Yönetimi

Bankalar yasalar gereği olası riskleri kapsamlı bir şekilde analiz etmek ve bunları azaltmak için önlemler almakla yükümlüdür. Bankalarda risk yönetimi, bankanın operasyonlarını ve varlığını etkileyebilecek potansiyel risklerin önlenmesi ve yönetilmesinde rol oynar. Kredi riski, piyasa riski, operasyonel risk, itibar riski, likidite riski gibi birçok risk türünün yönetilmesi için verinin toplanması, istatistiksel hesaplamaların yapılması, model oluşturulması ve raporlanması gerekmektedir.

RegTech çözümleri ilgili yasal gereklilikler ve banka içi uygulamalara dayalı olarak riskleri tanımlayan, değerlendiren ve izleyen otomatik sistemler oluşturarak uyumluluğu kolaylaştırabilir. Bu sistemler ilgili personelleri bilgilendirebilir ve bir tetikleyici olayın meydana gelmesi üzerine önceden tanımlanmış eylemleri otomatik olarak gerçekleştirebilir. Örneğin, belirli limitler veya risk seviyeleri aşıldığında kullanıcıyı uyarabilir ve/veya önceden programlanmış bir dizi adımla devam edebilir (Toronto Centre, 2017: 9).

RegTech'in iyileştirebileceği bir diğer önemli risk yönetimi işlevi ise risk modelleme ve tahmindir (Institute of International Finance, 2016: 8-9; Financial Stability Board, 2017: 18). Bankaların gelecekteki olası kayıp ve ihtiyaçları tahmin edebilmeleri ve senaryo analizleri yapabilmeleri için modelleme ve analitik araçlar kullanmaları gerekmektedir. Veri yönetimi, risk değerlendirmesi ve risk raporlama

dahil olmak üzere çeşitli risk yönetimi işlevleri için RegTech yazılımları kullanılabilir (Hugé, Duprel ve Pescatore, 2017: 4).

3.3.4. Yasal Raporlama

Yasal raporlama (Regulatory Reporting), bankaların BDDK, TCMB, MASAK gibi yasal otoritelere belirli aralıklar ile zorunlu olarak veri sunmasıdır. Bankalar istenen verileri düzenleyici kurumlara raporlayarak sektörün ve bankanın likidite yönetimi, aktif pasif yönetimi, kredi ve mevduat bilgisi gibi finansal sağlığı hakkında genel bir bilgi vermiş olur. Düzenleyici kurum raporları analiz ettikten sonra aşırı derecede riske maruz kalan bir banka veya sistemik risk tespit ederse risk gerçekleşmeden önce hafifletici önlemler uygulayabilir.

Bankalar düzenleyici kurumlara günlük, haftalık, aylık ve yıllık olmak üzere birçok konuda raporlama yapmak zorundadır. Raporlama sürecinde kullanılan eforun yanı sıra raporda belirtilen bilgilerin doğruluğu da çok önemlidir. Yanlış yapılan raporlama sonucunda bankanın ceza alması olasıdır. Bu sebeple bankalarda raporlama süreçlerinin otomatikleştirilmesi ve RegTech çözümlerinin uygulanması hem maliyet hem de kaynakların verimli kullanılması için doğru bir uygulama olacaktır.

3.3.5. İşlem İzleme

AML yönetmeliği uyarınca bankalar herhangi bir şüpheli veya yasa dışı faaliyeti tespit etmek için işlemleri izlemek (Monitoring & Screening) zorundadır. Bankaların bunu yapabilmesi için işlemlerin meta verilerini analiz etmesi, olası uyumsuz işlemleri belirlemesi, işaretlemesi ve raporlaması gerekmektedir. Tek bir global ödeme standardının olmaması da verilerin yorumlanmasını zorlaştırmaktadır (Institute of International Finance, 2017: 13).

Bankalarda geleneksel olarak işlemlerin taranması yapılmadıktan sonra şüpheli hareketler vaka bazında incelenir ve daha sonra ilgili yerlere raporlanır. AML süreçleri büyük ölçüde manuel olarak yapılmaktadır. Bankalar önlemlerini sertleştirdiği zamanlarda çok sayıda yanlış uyarıdan sorumlu olabilmektedir (Deloitte, 2018a: 7). Bu yanlış uyarılar zaman kaybına ve maliyete neden olmaktadır.

RegTech yazılımları kullanılarak işlemler daha hızlı ve doğru bir şekilde analiz edilerek izlenebilmektedir. Yazılımlarda işlem verileri müşterinin bilgileri ve geçmiş

işlem bilgileriyle analiz edilerek dolandırıcılık riski kapsamlı bir şekilde değerlendirilmekte ve şüpheli işlemler daha etkin bir şekilde tespit edilmektedir. RegTech yazılımları çok büyük boyutlardaki işlem verisini tarayabildiği için hem kaynaktan hem de zamandan tasarruf edilmiş olur.

3.4. Dijital Bankacılık Çağı

Dijital bankacılık geleneksel bankacılık işlemlerinin dijital kanallar yoluyla gerçekleştirilmesi olarak tanımlanabilir (Kurnia v.d., 2010: 1).Bankacılık sektöründeki gelişmelere bakıldığında; ATM'lerin (Automated Teller Machine) hayatımıza girmesi, POS (Point of Sale) makineleri, banka ve kredi kartları, NFC (Near Field Communication) teknolojisi ile kredi kartlarında temassızlık özelliği, mobil ve internet bankacılığı gibi gelişmeler bankacılık işlemlerini gerçekleştirme konusunda hayatımızı kolaylaştırmıştır. Günümüzde yaşanan teknolojik gelişmeler ile işlemlerin dijital kanallar yoluyla yapılabilmesi banka şubelerine olan ihtiyacı azaltmış ve şubesiz bankacılık kavramını ortaya çıkarmıştır. Türkiye'de çeşitli banka ortaklıkları ile kurulan Enpara, Cepteteb, Nuvo, Dijital Deniz gibi şubesiz dijital bankacılık uygulamalarına örnek gösterilebilir (Bozan, 2022). BDDK'nın 29 Aralık 2021 tarihinde yayımladığı "Dijital Bankaların Faaliyet Esasları ile Servis Modeli Bankacılığı Hakkında Yönetmelik"ten sonra kuruluş iznini alan ilk şubesiz dijital banka Hayat Katılım Bankası olmuştur (Fintech İstanbul, 2022c). Bankacılık alanında yaşanan gelişmeler aşağıdaki bölümlerde açıklanmıştır.

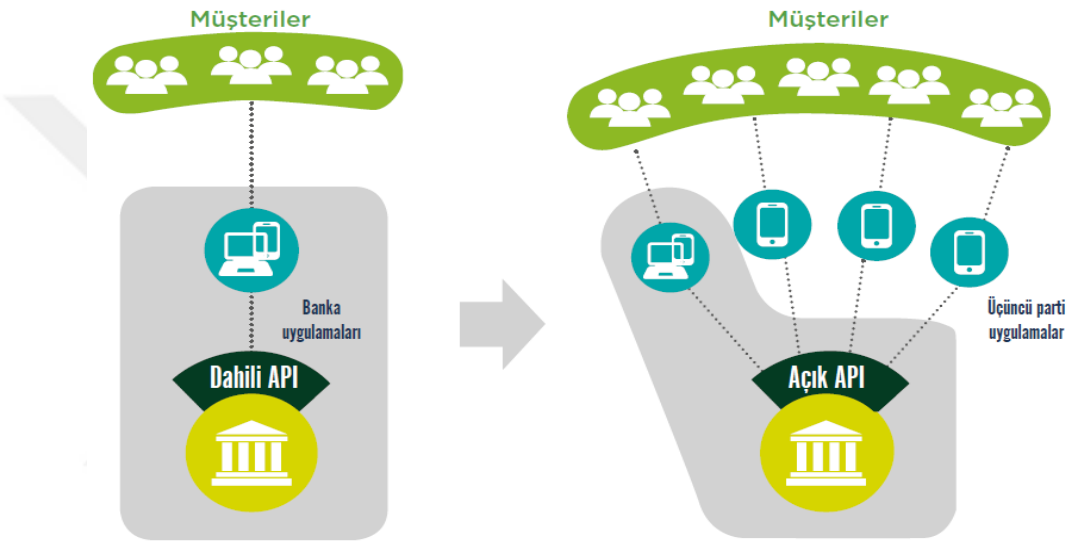
3.4.1. Açık Bankacılık

Finansal teknolojilerin gelişmesi geleneksel bankacılığın değişmesine ve yeni fırsatlara doğru evrilmesine yol açmıştır. Finansal hizmetler alanında yenilikçi çözümler ve daha iyi hizmet sunan FinTech oluşumlarının çıkması bankacılık sektörünü de hareketlendirmiştir.

Açık Bankacılık ya da Open Banking üçüncü taraf hizmet sağlayıcıların bankacılık işlemlerine ve müşteri verilerine daha iyi hizmet sağlamaları için API'ler (uygulama programlama arayüzleri) aracılığıyla erişimine izin veren bir sistemdir. Açık Bankacılık İngiltere Rekabet ve Piyasa Kurumu (CMA) ve Avrupa Bankacılık Otoritesi (EBA) tarafından finansal hizmetler alanına rekabetin getirilmesi için

tasarlanmış, PSD1 ve PSD2 (Payment Services Directive) düzenlemeleri ile finansal kurumların elinde tuttuğu verilerin üçüncü taraf hizmet sağlayıcıları ile paylaşılması zorunlu tutulmuş ve bankacılık API'ler ile açık bir sisteme evrilmiştir (Şahin ve Cantürk, 2020: 176). Türkiye'de ise BDDK tarafından 15 Mart 2020 tarihinde yayımlanan "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" ile açık bankacılık kavramı resmi olarak tanımlanmıştır.

Şekil 3.3 : Geleneksel Bankacılık ve Açık Bankacılık Modelleri



Kaynak: Fintech İstanbul, 2019: 9

Şekil 3.3'te geleneksel bankacılık ile açık bankacılık modellerinin işleyiş şekilleri karşılaştırılmıştır. Geleneksel bankacılıkta müşteriler bankadaki mevduat hesaplarına ve bilgilerine sadece ilgili bankanın mobil ve internet bankacılığı üzerinden erişebilmektedir. Açık bankacıkta ise bankalar API'lerini açık kaynak kodlu olarak diğer kurumlara açarlar ve müşteriler de finansal bilgilerin üçüncü taraflar ile paylaşılmasına izin vererek farklı bir uygulama üzerinden tüm hesap bilgilerine ulaşabilmektedir.

Bankaların API'ler üzerinden verilerini diğer hizmet sağlayıcılar ile paylaşması diğer firmalar ile iş birliğinin artmasını sağlamıştır. Sonuç olarak müşterinin çıkarına olan bu durum sektörde rekaberlik (iş birliği içinde rekabet) kavramını ortaya çıkarmıştır (Fintech İstanbul, 2019: 12). Rekaberlik sayesinde müşteriler daha geniş bir hizmet yelpazesine ulaşabilmektedirler.

Tablo 3.1 :Türkiye Açık Bankacılık Açık Kaynak API listesi

	Eylül 2019	Şubat 2020	Ağustos 2020	Aralık 2020	Şubat 2021	Temmuz 2021	Temmuz 2022
DenizBank	203	271	372	398	433	466	483
AktifBank	0	0	0	0	0	0	232
Albaraka	29	33	36	36	49	64	106
Kuveyt Türk	75	75	79	81	86	86	94
Vakıfbank	8	22	23	29	29	67	82
İş Bankası	31	31	34	37	41	46	56
Yapı Kredi	56	56	56	56	56	56	56
Akbank	9	9	9	10	13	13	29
Fibabanka	0	0	0	0	0	0	25
QNB Finansbank	0	0	5	9	17	20	20
Garanti Bankası	3	3	9	9	14	16	16
Ziraat Katılım	0	0	0	10	11	11	11
Vakıf Katılım	0	0	0	0	0	0	7
Ziraat Bankası	0	0	0	0	0	0	5

Kaynak: BirAPI aktaran Fintech İstanbul 2022

Tablo 3.1.'de Türkiye'deki bankaların açık kaynak kodu olarak paylaştıkları API sayıları görülmektedir. Yıllar içinde düzenlemenin gündeme geldiği Eylül 2019 tarihinden Temmuz 2022 tarihine kadar bankaların açtıkları API sayılarında büyük bir artış yaşanmıştır. Bu artışa rağmen her bankanın aynı oranda API'lerini açmadıkları görülmekle birlikte açık bankacılığın benimsenmesinin zaman alacağı söylenebilir.

3.4.2. Servis Bankacılığı

Servis Bankacılığı ya da Banking-as-a-Service (Baas) bankaların veya finans kuruluşlarının hizmet ve ürünlerini üçüncü taraf firmalara sağladığı ve onların da bu hizmetleri müşterilerine sunduğu bir modeldir. Bu model firmaların kendi finansal altyapılarını kurmak veya bankacılık lisansı almak zorunda kalmadan finansal ürün ve hizmetler sunmalarına olanak tanımaktadır. BaaS ile firmalar, üçüncü taraf bir sağlayıcının bankacılık altyapısını kullanırken müşterilerine sanal bankacılık, dijital cüzdanlar ve ödeme işleme gibi özellikler sunabilir.

Servis Bankacılığı sistemi açık bankacılıkta olduğu gibi API'leri kullanarak çalışmaktadır. Bankalar, çekirdek sistemlerini üçüncü taraf firmalara bağlamak için API'leri kullanır ve finansal ürün ve hizmetlere gerçek zamanlı olarak erişmelerini sağlar. Üçüncü taraf sağlayıcılar daha sonra bu API'leri kendi finansal ürünlerini ve

hizmetlerini oluşturmak ve müşterilerine sunmak için kullanabilir. İşletmeler, API'leri kullanarak pahalı ve zaman alıcı olabilecek kendi finansal altyapılarını geliştirmeye gerek kalmadan müşterilerine bankacılık hizmetleri sunabilir.

Türkiye'de BDDK'nın 29 Aralık 2021 tarihinde yayımladığı "Dijital Bankaların Faaliyet Esasları ile Servis Modeli Bankacılığı Hakkında Yönetmelik" (BaaS Yönetmeliği) ile birlikte resmiyet kazanmıştır.

Servis bankacılığı zaman zaman açık bankacılık ile karıştırılabilmektedir. İkisinin faaliyetleri benzer olsa da birbirinden farklıdır. İkisinin arasındaki temel fark, API'lerin nasıl kullanıldığı ile ilgilidir. Servis bankacılığı bankacılık işlevlerine erişmek için API'leri kullanırken açık bankacılık tüketici verilerine erişmek için API'leri kullanmaktadır. Diğer bir farklılık ise açık bankacılık genellikle bankalar ve finans kurumları tarafından yeni hizmetler sunmak ve yeni gelir akışları oluşturmak için kullanılırken servis bankacılığı Fintech gibi banka dışı firmaların müşterilerine finansal hizmetler sunmak için kullandıkları bir iş modelidir.

3.4.3. Neobankalar

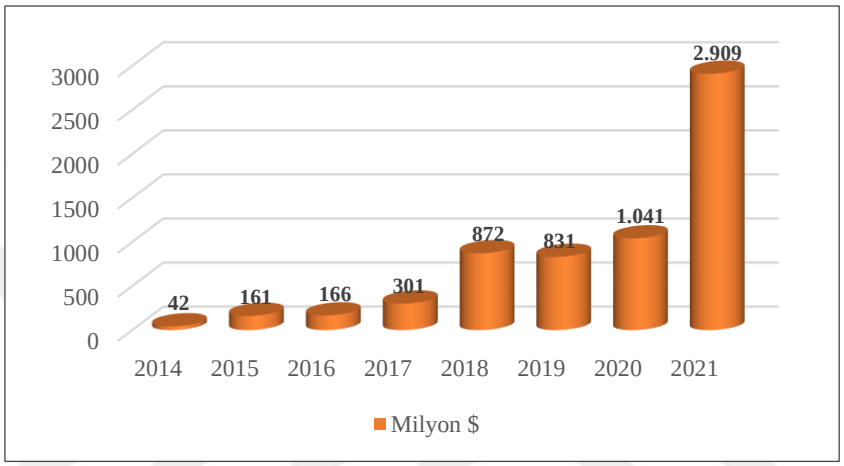
Neobankalar tamamen çevrimiçi faaliyet gösteren ve mobil uygulamalar veya web platformları aracılığıyla bankacılık hizmetleri sunan finansal kuruluşlardır. Geleneksel bankaların aksine, Neobankaların daha verimli çalışmalarına ve müşterilere daha rekabetçi oranlar ve ücretler sunmalarına olanak tanıyan fiziksel şubeleri yoktur (Bilham, 2022). Ayrıca Neobankaların kendilerine ait bir bankacılık lisansı olmadığı için müşterilerden mevduat toplayamaz ve kredi veremezler (Chang, 2023). Para için emanetçi görevi gören geleneksel bir bankayla uyum ve KYC kontrollerini sağlayarak mobil öncelikli bir deneyim sunarlar (Alvantia, 2018). Neobankalara örnek olarak Revoult, Chime, Aspiration gösterilebilir.

3.4.4. Rekabetçi Bankalar

Rekabetçi (Challenger) bankalar, bireysel bankacılığı dijitalleştirmek ve modernize etmek için yazılımlardan yararlanan, bankacılık lisansına sahip teknoloji firmaları olup Birleşik Krallık'ta Big-Four bankalarına (Barclays, Lloyds, HSBC ve RBS) meydan okumak isteyen herhangi bir bankayı tanımlamak için kullanılmaktadır (Sarac, 2020).

Challenger bankalar geleneksel bankacılıktaki operasyonel maliyetlerden ve karmaşıklıktan kaçınarak düşük maliyet ile hizmet sunabilmekte ve geleneksel bankaların eski teknoloji sistemleri nedeniyle ihmal edilen alanlardan da faydalanabilmektedir (Sarac, 2020).

Grafik 3.3 :2014-2022 yılları arasındaki Challenger Bankaların Sermaye Fonlamaları



Kaynak: CBinsight, 2022

Grafik 3.3'te Avrupa menşeli rekabetçi bankaların 2014 yılından bu yana 6 milyar $'dan fazla finansman çektiği ve artarak devam ettiği görülmektedir. 2014-2021 yılları arasında neredeyse 70 kat artması göz önünde bulundurulduğunda dijital bankacılığın gelişmesiyle birlikte bu oran daha da artacaktır.

3.5. RegTech ve Bankacılık İlişkisi

Bankacılık sektöründe uyum gerekliliklerinin giderek daha karmaşık ve karşılanması maliyetli hale gelmesiyle uyum riskinin yönetiminde yeni arayışlar başlamıştır. RegTech ve bankacılık arasındaki ilişki de bankaların mevzuat uyumluluğunu daha verimli ve etkili bir şekilde yönetmeye çalıştıkları için son yıllarda giderek daha önemli hale gelmiştir.

RegTech, bankacılık sektörüne maliyet tasarrufu, artan verimlilik ve iyileştirilmiş risk yönetimi dahil olmak üzere birçok fayda sunmaktadır. RegTech çözümleri, uyumluluk süreçlerini kolaylaştırarak ve manuel girdi ihtiyacını azaltarak bankaların verimliliğini artırmasına yardımcı olurken personelin zamanını verimli

kullanmasını ve genel üretkenliği artırmasını da sağlar. Ayrıca RegTech yazılımları bankalara daha iyi veri analitiği ve izleme çözümleri sağlayarak bankanın risk yönetimini de geliştirir. Böylece bankalar hileli faaliyetleri ve mali suç yöntemlerini tespit etme ve önlemede daha başarılı sonuçlar almış olur.

RegTech çözümlerinin faydalarına rağmen bunların uygulanmasında zorluklar da bulunmaktadır. Bunlardan bir tanesi etkili RegTech çözümleri geliştirmeyi zorlaştırabilecek düzenleyici gerekliliklerin ve mevzuatların karmaşık olmasıdır. Bu karmaşıklık nedeniyle firmalar yazılımlarına daha fazla yatırım yapmak zorunda kalmakta ve bu da finansal durumlarını etkilemektedir. RegTech çözümlerinin, zor ve maliyetli olabilen, hızla değişen düzenleyici ortama ayak uydurabilmesi gerekir. Diğer bir zorluk ise mevcut sistem ve süreçlerle entegrasyon ihtiyacıdır. Bankaların karmaşık BT altyapıları bulunmaktadır. Bu sebeple RegTech çözümlerinin etkili olabilmesi için bu sistemlerle sorunsuz bir şekilde entegre olabilmesi gerekir.

Teknolojinin gelişmesiyle birlikte Avrupa'da PSD2 düzenlemesiyle açık bankacılığın doğması RegTech 3.0 devrine geçişi hızlandırmış ve RegTech sektörünün gelişmesinde katkıda bulunmuştur. Açık bankacılık yoluyla elde edilen veriler, RegTech'in analiz edebileceği veri miktarını önemli ölçüde artırarak daha fazla doğruluk ve kapsamlılık sağlamakta ve otomasyon süreçleri, makine öğrenimi ve algoritmalar kullanılarak gerçek zamanlı olarak toplanıp analiz edilebilmektedir. Ayrıca açık bankacılık çok az kredi geçmişi olan veya hiç olmayan insanların verilerinin RegTech'e ulaşması için bir araçtır. Açık bankacılık verileri, kredi büroları tarafından saklanan eski mali geçmişlerden değil, doğrudan müşteri banka hesaplarından elde edildiği için RegTech, çok daha fazla miktarda veriyi ve müşteri profilini analiz ederek riskleri daha doğru bir şekilde belirleyebilmektedir (Ascent Regtech, 2023). Bu sebeplerle açık bankacılığın RegTech sektörünün gelişiminde büyük bir katkısı olduğu söylenebilir.

Sonuç olarak RegTech ile bankacılık arasındaki ilişki, bankaların mevzuata uyum sağlama şeklini dönüştürme potansiyeline sahip önemli bir ilişkidir. RegTech çözümleri, bankalara uyum riskinden kaynaklanan maliyetleri düşürme, verimliliği artırma ve uyum başarısızlıkları riskini azaltma yolu sunmaktadır. Bununla birlikte, RegTech çözümlerinin etkili ve güvenli olmasını sağlama ihtiyacı da dahil olmak

üzere, ele alınması gereken zorluklar da vardır. Uyum riski yönetiminde kullanılacak çözümlere yönelik artan talep ve RegTech endüstrisinde süregelen yeniliklerle RegTech ile bankacılık arasındaki ilişkinin geleceğinin parlak olduğu söylenebilir.

DÖRDÜNCÜ BÖLÜM
UYGULAMADA REGTECH

4. RegTech Uygulamaları ve Wells Fargo Vaka İncelemesi

Bankaların düzenlemelere uyum için katlandıkları maliyetlerin yanında uyumsuzluk sonucu yasal otoriteler tarafından verilen cezalar da bulunmaktadır. Ceza riskinin en aza indirilebilmesi için etkin bir uyum riski yönetimi ve denetimi yapılmalıdır. Çalışmanın bu bölümünde düzenlemelere uyum için katlanılan maliyetler ve uyumsuzluk sonucunda verilen cezalar araştırılmış, uyum riskinin bankaların operasyonel süreçleri içerisindeki yeri kapsamında Wells Fargo vakası incelenmiş ve RegTech firması örnekleri verilerek Türkiye'deki uyum konusu ve RegTech sektörü ele alınmıştır.

4.1. Uyum Maliyeti

Finansal istikrarı sağlamak, tüketicileri korumak ve finansal suçları önlemek için tasarlanan yasal düzenlemeler, bankacılık sektörünün önemli bir parçasıdır. Ancak bu düzenlemeler son yıllarda önemli ölçüde arttığı için bankalar üzerinde hem operasyonel hem de finansal açıdan yük oluşturmaktadır.

Bankaların uyum maliyeti (Regulatory Cost), maaşlar, yasal ücretler, teknoloji giderleri gibi doğrudan maliyetlerin yanı sıra düzenlemelere uyum için harcanan yönetim süresinin fırsat maliyeti gibi dolaylı maliyetleri de içermektedir.

Bankacılık sektöründe uyum maliyetlerinin artmasının sebeplerinden biri, bankaların uymak zorunda olduğu düzenlemelerin sayısının artmasıdır. 2008 mali krizinden sonra dünyanın dört bir yanındaki düzenleyiciler, krizin tekrarlanmasını önlemeyi amaçlayan bir dizi yeni düzenlemeleri uygulamaya koymuştur. Bu düzenlemeler de daha yüksek sermaye gereklilikleri, daha sıkı risk yönetimi uygulamaları ve daha kapsamlı raporlama gereklilikleri içerdiği için bankaların uyum maliyetlerini artırmıştır.

Başlangıç ve devam eden olmak üzere iki tür uyum maliyeti vardır. Başlangıç maliyetleri, bir düzenlemenin gerekliliklerine uymak için değişikliklerin

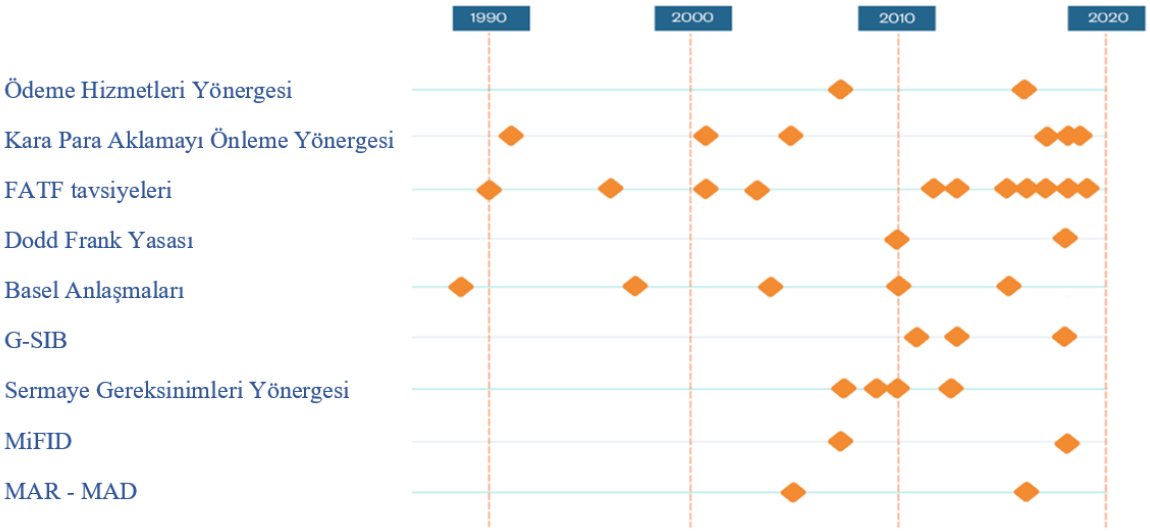
uygulanmasının bir kereye mahsus maliyetleridir. Örnek vermek gerekirse (Elliehausen, 1998: 3);

- Yönetmeliği yorumlamak, yöneticilere danışmanlık yapmak ve prosedür ve formları incelemek için yapılan yasal harcamalar,
- Prosedürlerin ve formların gözden geçirilmesi ve revize edilmesi, uyum faaliyetlerinin koordinasyonu ve iç denetim programlarının tasarlanması için yönetim giderleri,
- Eğitim giderleri,
- Bilgi sistemlerini değiştirme ve kayıtları saklama maliyetleri,
- Yazılımın programlanması ve test edilmesi için yapılan harcamalar,
- Yeni formlar tasarlama ve eskimiş formları yok etme maliyetleri.

Devam eden maliyetler ise bir yönetmeliğin gerektirdiği faaliyetleri gerçekleştirirken katlanılması gereken ve tekrar eden maliyetleridir. Örnek vermek gerekirse (Elliehausen, 1998: 3);

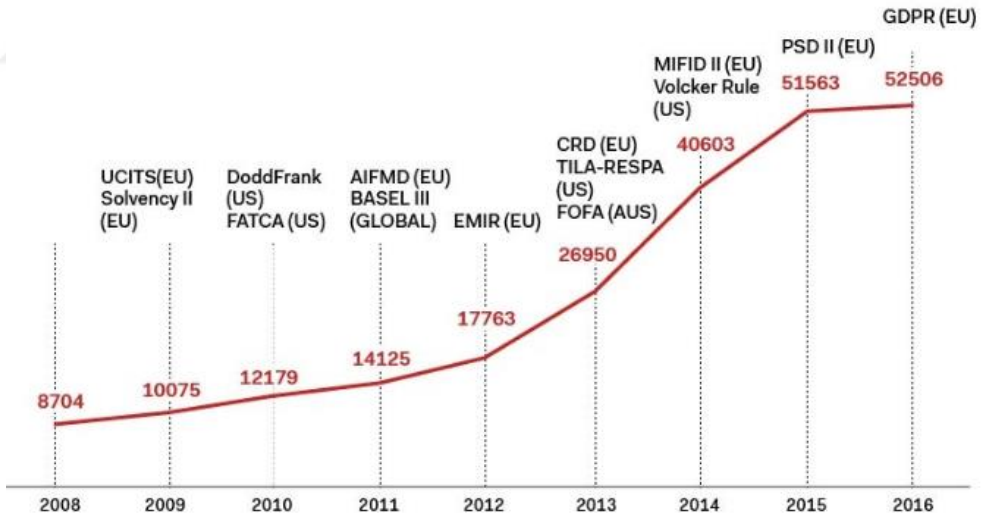
- Çalışanların uyumunu izlemek ve düzenleyici kurumlarla uyum incelemelerini koordine etmek için katlanılan yönetim giderleri,
- Raporların hazırlanması ve müşteri sorularının yanıtlanması için katlanılan personel giderleri,
- Şikayetleri incelemek için katlanılan yasal masraflar,
- Müşterilere yazılı açıklamalar sağlamak için katlanılan dijital ve posta masrafları.

Grafik 4.1: Tarihsel Olarak Yapılan Düzenlemeler



Kaynak: Prove, 2022

Grafik 4.2 :Yıllık Toplam Düzenleyici Yayın, Değişiklik ve Duyuru Sayısı



Kaynak: Prove, 2021

Grafik 4.1 ve Grafik 4.2'de yıllara göre artan düzenlemeler ve bunların yaklaşık sayfa sayıları belirtilmiştir. Her düzenleyici faaliyette finansal kurumların sürekli farkında olması gereken yüzlerce ve binlerce kural değişikliği vardır. Bu da uyum konusunda yaşanan herhangi bir aksiliğin finansal kurumlara milyarlarca dolara mal olabileceği anlamına gelmektedir. Her yeni çıkan düzenleme ile belgeler binlerce sayfa uzunluğunda olduğu için bankalar ve finansal kurumlar için (özellikle de çok

fazla kaynağa sahip olmayan daha küçük olanlar için) her birini kısa bir süre içinde gözden geçirmek, ilgili değişiklik ihtiyaçlarını belirlemek ve uyumlu kalmak için bu değişiklikleri süreçlerinde uygulamak zordur (Prove, 2021).

The Trade tarafından yayınlanan araştırmada bankaların yalnızca 2016 yılında yasal uyum için 100 milyar $'ın üzerinde harcama yaptığını (McDowell, 2017) ve bu maliyetin arttığı belirtilmiştir (Thomson Reuters, 2018: 5). Bain & Co., yönetişim riski ve uyum (GRC) harcamalarının "bankayı yönetme" maliyetinin %15-20'sini ve "bankanın değişim(proje)" maliyetlerinin %40'ını oluşturduğunu tahmin etmektedir (Memminger, v.d., 2016). Spesifik düzenlemelere bakıldığında örneğin 2018 yılına kadar Dodd Frank 36 milyar $'a, MiFID II ise 2,5 milyar avroya mal olmuştur (Butler ve O'Brien, 2019: 87).

Bankaların uyum maliyetlerinin bir bütün olarak endüstri üzerinde de etkileri bulunmaktadır. Örneğin küçük veya orta ölçekli bankaların katlandığı uyum maliyeti bilançolarında büyük ölçekli bankalarla kıyaslandığında daha fazla yer tutabilir. Bankalar da uyum maliyetini tüketicilere yansıtmaya çalıştıklarından, bu süreç müşteriler için artan ücretlerle sonuçlanabilir.

Tablo 4.1 :Bölgelere Göre Mali Suçlarda Uyum Maliyeti

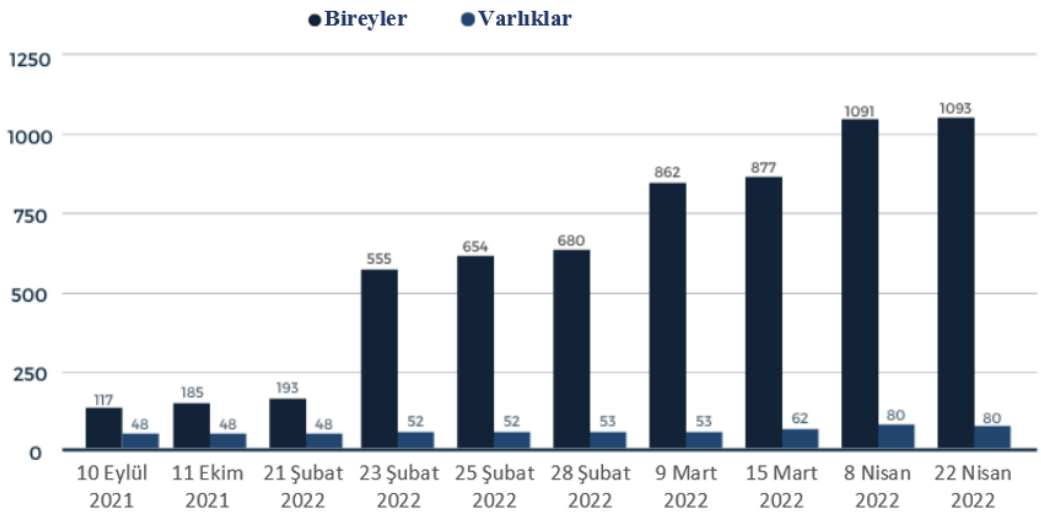
Ülke ve Bölgeler (Milyar $)	**2019**	**2020**	**Değişim Oranı**
Kuzey Amerika	31,50	42,00	33,33%
Amerika Birleşik Devletleri	*26,40*	*35,20*	*33,30%*
Kanada	*5,10*	*6,80*	*33,30%*
LATAM	4,50	5,90	31,10%
Brezilya	*3,01*	*3,98*	*32,20%*
Meksika	*0,71*	*0,90*	*26,80%*
Arjantin	*0,33*	*0,39*	*18,20%*
Şili	*0,31*	*0,50*	*61,30%*
Kolombiya	*0,15*	*0,18*	*20,00%*
Avrupa	87,00	102,50	20,90%
Almanya	*47,50*	*57,10*	*20,20%*
Fransa	*21,00*	*24,80*	*18,10%*
İtalya	*15,80*	*20,00*	*26,60%*
Hollanda	*2,70*	*3,30*	*22,20%*
Güney Afrika	2,30	3,30	43,50%
Güney Afrika Cumhuriyeti	*2,30*	*3,30*	*43,50%*
APAC	5,18	6,59	27,20%
Singapur	*3,10*	*3,80*	*21,70%*
Endonezya	*1,60*	*2,10*	*32,10%*
Filipinler	*0,48*	*0,69*	*43,80%*

Kaynak: LexisNexis, 2021: 10

LexisNexis tarafından piyasalarda ve çeşitli kuruluşlarda 1.015 mali suçlarda uyum yasal otoriteleri arasında kapsamlı bir anket gerçekleştirilmiş ve 2021 yılı "True Cost Of Financial Crime Compliance Study" raporu çıkarılmıştır (LexisNexis, 2021: 4). Tablo 4.1'de çeşitli ülkelerin 2019 ve 2020 yılı mali suçlarda uyum maliyetleri gösterilmiştir. İlgili tabloda ülkelere göre 2020 yılındaki uyum maliyetlerindeki artışın bir önceki yıla göre %18,10 ila %61,30 arasında değiştiği, her ülkenin uyum maliyetinin arttığı, Avrupa bölgesinin uyum maliyetinin 2020 yılında 102,5 Milyar $ ile global uyum maliyeti içerisinde büyük bir yere sahip olduğu görülmektedir, mikro açıdan bakarsak Almanya pazarı maliyetlerinin diğerlerini önemli ölçüde geri bıraktığı görülmektedir.

Ayrıca LexisNexis'in raporunda mali suçların kripto para birimi ve siber dolandırıcılık nedeniyle attığı, daha fazla kurumun yalnızca artan mali suç risklerinden değil aynı zamanda daha sert cezalar içeren düzenlemelerin getirdiği durum tespiti zorluklarıyla karşı karşıya kaldığı, RegTech'in (İlgili raporda "uyumluluk teknolojisi" olarak belirtilmiştir) farklı beceri düzeyleri ve yılların deneyimine sahip uyumluluk profesyonellerini tamamlamak ve desteklemek için gerekli ve değerli bir kaynak olduğu, RegTech çözümlerine yatırım yapan finans firmalarının yeni ve ani değişikliklerle başa çıkmak için daha hazırlıklı olacağı belirtilmiştir (LexisNexis, 2021: 41-42).

Grafik 4.3 : Rusya Savaşı Nedeniyle Avrupa Birliği Yaptırımlarının Kümülatif Sayısı



Kaynak: Statistica, 2023

Grafik 4.3'te hızla artan düzenlemelere uyum konusunda örnek olması amacıyla Ukrayna-Rusya savaşı nedeniyle Rusya'ya karşı kişi ve kuruluşlara yönelik tarihlere göre Avrupa Birliği yaptırımlarının kümülatif sayısı gösterilmiştir. İlgili grafikte çok kısa süre içerisinde yapılan toplam düzenlemelerin 6 kattan daha fazla arttığı göz önüne alınırsa, hızla artan düzenlemelere çok kısa sürede ve minimum hata ile uyum sağlanması önem arz etmektedir. RegTech çözümleri de finansal firmaların bu düzenlemelere hızla uymasını ve uyum risklerini düşürmelerinde yardımcı olacaktır.

4.2. Uyum Cezaları

Bankalar çok çeşitli yasalara yönetmeliklere ve standartlara uymak zorunda olduğu için üst düzeyde denetime tabi kurumlardır. Bu gerekliliklere uyulmaması, banka için önemli mali, yasal ve itibari sonuçlara yol açabilir. Bankalar için en ağır sonuçlardan biri de düzenleyici otoriteler tarafından para cezalarının verilmesidir.

Bankalar, yasa ve yönetmeliklere uyulmaması, kötü yönetişim uygulamaları, kişisel verilerin kişinin rızası dışında işlenmesi ve paylaşılması, AML/KYC süreçleri, yetersiz risk yönetimi ve operasyonel süreçler dahil olmak üzere çeşitli nedenlerle para cezasına çarptırılabilir. Düzenleyici makamlar, bankaları uyumluluk ve risk yönetimi

uygulamalarını iyileştirmeye teşvik etmek ve gelecekteki ihlalleri caydırmak için para cezaları uygular.

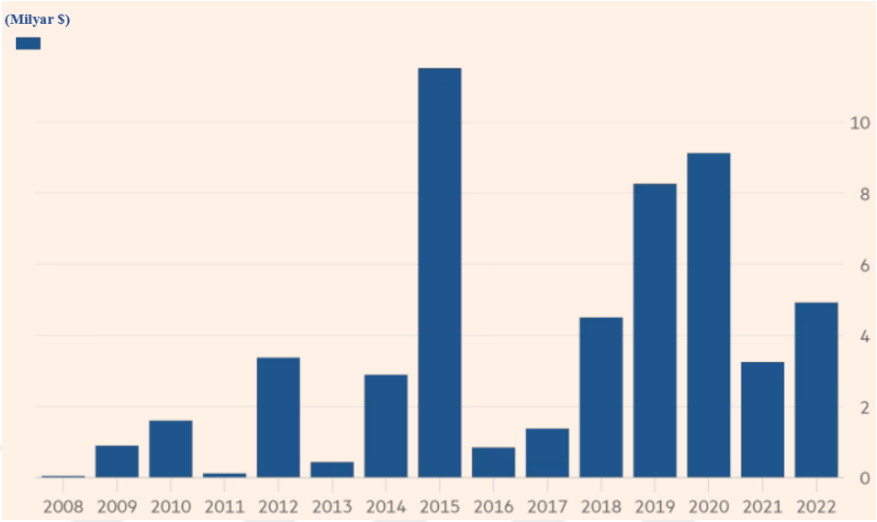
Bankalara uygulanan para cezasının miktarı ihlalin ciddiyetine, bankanın büyüklüğüne ve ihlal sayısına göre değişmektedir. İhlal nedeniyle bankaya kesilen ceza haricinde ihlalde payı oldukları tespit edilen bankaların üst düzey yöneticilerine veya yönetim kurullarına da para cezası uygulanabilmektedir.

Para cezaları kazançlarda önemli bir azalmaya neden olabileceği gibi bankanın hisse senedi fiyatında düşüşe yol açabilir ve bankanın finansal performansı üzerinde önemli bir etkiye sahip olur.

Bankalar için kesilen para cezalarının mali boyutlarının yanında diğer sonuçları da bulunmaktadır. Müşteri güveni kaybı ve itibarın zedelenmesi bunlardan birkaçıdır. Müşteri güveninin zedelenmesi ve itibar kaybı bankada müşteri kaybına, olası mevduat çıkışlarına ve mevduat toplamada yani kaynak bulmada sıkıntılara yol açabilir. Bu da bankaların likidite sorunu yaşamasına hatta bankanın batmasına bile neden olabilir. 1741'de kurulan İsviçre'nin en eski özel bankası Wegelin & Co, ABD'nin zengin bazı kişilerin hesaplarını offshore hesaplarda gizlemesi ve en az 1,2 milyar $'lık vergi ödemelerinden kaçmasına yardım etmekle suçlanmış ve suçunu kabul etmiştir. Banka, ABD yasal otoritelerine 57,8 milyon $ para cezası ve tazminat ödemeyi kabul ettikten sonra faaliyetlerini durduracağını duyurmuştur (Raymond, ve Browning, 2013).

Para cezaları bankaların düzenlemelere uyumu sağlamak için yeni politikalar ve prosedürler uygulamasına, operasyonel süreçlerinde değişikliklere gitmesine, zaman alıcı denetimlerin armasına ve böylece bankanın ek maliyetlerinin artmasına neden olabilir.

Grafik 4.4 : Global AML Kaynaklı Ceza Tutarları



Kaynak: Noonan ve Smith, 2023

Grafik 4.4'te 2008 krizinden günümüze AML kaynaklı uygulanan para cezaları gösterilmiştir. Genelde para cezaları ihlal yapıldıktan sonraki yıllarda verildiği için 2022 yılında Ukrayna-Rusya savaşı nedeniyle çıkarılan yaptırımların ihlalleri dahil edilmemiştir. Küresel ölçekteki AML cezaları, bildirilen 3.495 olay sonucunda 2022'de bir önceki yıla göre %50'lik bir artış kaydederek yaklaşık 5 milyar $'a ulaşmıştır (Fineksus, t.y.(b)). Böylece 2008 küresel krizden bu yana toplamda neredeyse 55 milyar $ finansal kurumların kara para aklamayı önleme düzenlemeleri sebepli maliyete katlandıkları anlamına gelmektedir.

Aşağıdaki Tablo 4.2'de çeşitli bankalara yıllara ve konularına göre verilen cezalar gösterilmiştir.

Tablo 4.2 : Banka Cezaları

Banka Adı	Ceza Tutarı	Kurum	Konu	Tarih
Deutsche Bank	9,8 Milyon $	BaFin	Kontrol Eksikliği	2021
Societe Generale Group	1,4 Milyar $	Çeşitli ABD Otoriteleri	Ambargo İhlali	2018
JPMorgan Chase & Co.	200 Milyon $	SEC, CFTC	Personel İletişim Hataları	2021
Standard Chartered Bank	61,5 Milyon $	BoE	Likidite pozisyonunun yanlış raporlanması	2021
Santander UK	132 Milyon $	FCA	AML	2022
Wells Fargo	97,8 Milyon $	FED ve OFAC	Yaptırım İhlalleri	2023

Kaynak: Comfort, ve Arons, 2021; Johnson, v.d., 2018; Levitt ve Bain, 2021; Wilson, 2021; Bodoni ve Browning, 2022; Lang, 2023

i. Deutsche Bank cezası

BaFin, 28 Aralık 2021'de Deutsche Bank AG Avrupa Kıyaslama Yönetmeliği'nde (the European Benchmarks Regulation) belirtilen EURIBOR ile ilgili etkili önleyici sistemlere, kontrollere ve politikalara sahip olmadığı için 9,8 milyon $ tutarında idari para cezası vermiştir (BaFin, 2021).

İlgili yönetmeliğin amacı geçerli ölçütler sağlamak ve manipülasyonu önlemek olduğu için katkıda bulunan paydaşların etkili sistemlere ve kontrollere sahip olmasını gerektirir. Deutsche Bank, 2015 yılında gösterge faiz oranlarını manipüle etme girişimleri nedeniyle ABD ve Birleşik Krallık otoritelerine 2,5 milyar $ para cezası ödemeyi kabul ettiği skandal sonrasında hala ceza alması, verdiği taahhütleri tam olarak yerine getirmediğini göstermiştir (Comfort ve Arons, 2021).

ii. Societe Generale Group cezası

Fransa'nın en büyük bankası olan Societe Generale 2018 yılında ABD yasal otoriteleri tarafından ABD'nin Küba ve diğer ülkelere yönelik yaptırımlarını ihlal etmesi nedeniyle bankaya 1,4 milyar $ ceza verilmiştir (Johnson, v.d. 2018).

Para cezaları Amerikan Merkez Bankası (Federal Reserve), ABD Adalet Bakanlığı (U.S. Department of Justice), ABD Hazine Bakanlığı Yabancı Varlıklar Kontrol Ofisi (the U.S. Treasury's Office of Foreign Assets Control), New York Bölge Savcılığı ve New York Mali Hizmetler Departmanı tarafından verilmiştir. Amerikan yetkililer, bankanın 2003'ten 2013'e kadar İran, Sudan, Küba ve Libya da dahil olmak üzere ambargoya tabi olan veya ABD tarafından başka bir şekilde yaptırım uygulanan ülkelerdeki taraflara milyarlarca dolarlık yasa dışı işlem gerçekleştirdiğini belirtmiştir.

2021 yılında yer alan habere göre banka CEO'su Frederic Oudea'nın milyarlarca dolar uyum cezası ödedikten sonra bankanın yasal işlerinin yönetimi üzerinde daha fazla kontrol sahibi olmak için bankanın risk ve uyum işlevlerini devraldığı belirtilmiştir (Rajbhandari, 2021). Banka CEO'ları genelde uyum ve risk gibi ayrı işlevlerin doğrudan kontrolünü nadiren üstlenmekte ve bu görevi vekillerine devretmektedir fakat Oudea'nın bu görevi üstlenmesi uyum riski yönetiminin banka için ne kadar önemli olduğunu ve yönetilememesi durumunda bankanın büyük sorunlar yaşayabileceğini göstermiştir.

iii. JPMorgan Chase & Co. Cezası

JPMorgan Chase & Co, zorunlu olarak tutulması gereken kayıtları tutmadığı için 17 Aralık 2021 tarihinde SEC tarafından 125 milyon $ (SEC, 2021), Emtia Vadeli İşlemleri Ticaret Komisyonu (The Commodity Futures Trading Commission) tarafından da 75 milyon $ (CFTC, 2021) olmak üzere toplam 200 milyon $ para cezası verilmiştir.

İlgili kararda banka üst düzey yöneticilerinin de dahil olduğu banka çalışanlarının kişisel mesaj ve Whatsapp mesajları dahil olmak üzere onaylanmamış kanallar üzerinden hem dahili hem harici olarak müşteriler ile iletişim kurduğu, bu mesajların CFTC tarafından zorunlu olarak tutulması gereken kayıtlar kapsamında olduğu, bu mesajların JPMorgan tarafından muhafaza edilmediği ve istendiğinde CFTC temsilcisine sunulamadığı belirtilmiştir (CFTC, 2021).

iv. Standard Chartered cezası

İngiltere Merkez Bankası (BoE) Standard Chartered Bank'a likidite pozisyonunu yanlış raporladığı ve süreçteki kontrol eksikliği nedeniyle 17 Aralık 2021 tarihinde 61,51 milyon $ para cezası verilmiştir (BoE, 2021: 1).

Bankacılık otoriteleri, bankaların aniden çok sayıda para çekme talebiyle karşı karşıya kalmaları durumunda yeterli nakit veya nakit benzeri varlıklara sahip olduklarından emin olmak için bankaların likidite pozisyonlarını izlemektedir. Otoriteler bu pozisyonları bankaların kendilerine gönderdiği belirli standartta raporlar aracılığıyla gerçekleştirmektedir. İngiltere Merkez Bankası, Standard Chartered'ın Mart 2018 ile Mayıs 2019 arasında likidite metriğini bildirirken beş hata yaptığını, hatalardan birinde bankanın likidite pozisyonunu 7,9 milyar $ fazla bildirilmesiyle sonuçlandığını, diğer bir hatanın likidite raporlaması için kullanılan bir elektronik tablodaki bir hücrenin sıfır veya negatif bir değer beklendiği halde pozitif bir değere sahip olmasından kaynaklandığını belirtmiştir (Ramnarayan, 2021).

v. Santander UK

Santander UK bankasına yüz milyonlarca sterlinlik şüpheli fonları izlemesine ilişkin bir dizi yanlış adım da dahil olmak üzere tekrarlanan kara para aklamayı önleme

başarısızlıkları nedeniyle 9 Aralık 2022 tarihinde FCA tarafından 108 milyon £ (132 milyon $) para cezası verilmiştir (FCA, 2022).

FCA yaptığı açıklamada Santander'in 31 Aralık 2012 ile 18 Ekim 2017 tarihleri arasında AML sistemlerini gerektiği gibi denetleyip yönetemediğini, böylece 560.000'den fazla ticari müşterisinin hesap gözetiminin önemli ölçüde etkilendiğini, bankanın müşterilerinin yapacakları iş hakkında sağladıkları bilgileri yeterince doğrulamak için etkisiz sistemlere sahip olduğunu ve müşterilerin hesaplarından geçeceklerini söylediği para ile gerçekte yatırılan parayı kıyaslama ve izlemede başarısız olduğunu belirtmiştir (FCA, 2022). Santander 2017 yılından sonra süreç ve sistemlerini yeniden yapılandırmaya karar vermiştir (Bodoni ve Browning, 2022).

vi. Wells Fargo

Amerikan yasal otoriteleri 30 Mart 2023 tarihinde yaptıkları açıklamada Wells Fargo'nun ABD'nin İran, Suriye ve Sudan'a yönelik yaptırımlarının açık bir şekilde ihlal edilmesini sağlayarak uyum risklerini yönetememesi nedeniyle yaklaşık 97,8 milyon $ para cezası ödeyeceğini açıklamıştır (Lang, 2023). Bu cezanın 67,8 milyon $'lık kısmı FED, geri kalan 30 milyon $'lık kısmı da Yabancı Varlıkları Kontrol Ofisi (OFAC-the Treasury Department's Office of Foreign Assets Control) tarafından verilmiştir.

OFAC yaptığı açıklamada, Wells Fargo ve Wells Fargo'nun 2008 yılında satın aldığı Wachovia Bank'ın bir Avrupa bankasına Eximbills adlı finansal yazılım platformu sağladığı, bu platformun da yaptırım uygulanan İran, Sudan ve Suriye'deki kişi ve bölgelerde 27 Aralık 2010 ile 7 Aralık 2015 arasında meydana gelen 532 milyon $'lık 124 işlemi işleyerek yaptırımları ihlal ettiği, bankanın uzun yıllar boyunca bariz ihlalleri tespit edememesinin risk değerlendirme ve gözetim mekanizmalarındaki eksikliklerden kaynaklandığı belirtmiştir (OFAC, 2023: 1).

Verilen cezalar bu tür ihlallerin kasıtsız ve dolaylı olduğu kabul edilse bile yasal otoritelerin potansiyel yaptırım ihlallerini şiddetle takip ettiğini göstermektedir. Bu nedenle bankalar yaptırımları takip ederek prosedür ve süreçlerini güncel tutmalı, gerektiğinde bu alanlarda yatırım yapmalı ve cezalardan kaçınmak için uyum risklerini etkin şekilde yönetmelidir.

4.3. Uyum Riskinde Proaktif Uygulamalar ve Wells Fargo Vakası

AML/KYC gibi süreçlerin yanında operasyonel süreçler nedeniyle bankalar uyum riskine maruz kalabilmektedir. Bankaların uyum riskinin etkin yönetilememesi neticesinde potansiyel zarar kaybına uğramamaları için proaktif uygulamalar geliştirmesi gerekmektedir.

4.3.1. Bankacılıkta Operasyonel Risk

Bankacılıkta operasyonel süreçler, bankaların günlük operasyonlarının kritik bir bileşenidir. Hesap açma ve kapatma, kredi verme, ödeme işlemleri gibi birçok işlemi, müşteri ilişkilerini ve risk yönetimi dahil olmak üzere çok çeşitli faaliyetleri kapsarlar. Bankadaki operasyonların sorunsuz işlemesini sağlamak için operasyonel süreçlerin verimli, güvenilir ve yasal gerekliliklerle uyumlu olması gerekmektedir.

Operasyonel süreçlerin iyi yönetilmesi bankanın hem finansal hem de itibari değerine olumlu katkıda bulunmaktadır. Örneğin, operasyonel süreçleri etkin yönetilen bankaların yüksek kaliteli hizmet ve destek sunması müşteri memnuniyetini ve sadakatini artırabilir. Bu da bankanın müşteri kazanmaya devam ederek daha fazla kar etmesini ve müşteri memnuniyetini yükselterek de bankanın piyasadaki itibarını artırmayı sağlamaktadır.

Bankaların süreçlerini yönetirken ele alması gereken çeşitli riskler bulunmaktadır. Finans sektöründeki geleneksel yaklaşımda üç temel risk kategorisi tanımlanır: kredi riski, likidite riski ve piyasa riski. Bu riskler altı türe ayrılabilir: sistematik veya piyasa riski, kredi riski, karşı taraf riski, likidite riski, operasyonel risk ve yasal risk (Santomero, 1997: 88). Bankacılık sektöründe, dolandırıcılık vakalarının Barings bankasının iflasına ve Daiwas Bank'ın 1 milyar $ zarara yol açtığı bu tür popüler vakaların ardından 1990'ların sonlarından itibaren operasyonel riske dikkat çekilmiştir.

Operasyonel risk, yetersiz veya başarısız dahili süreçler, insanlar ve sistemlerden veya harici olaylardan kaynaklanan kayıp riski olarak tanımlanabilir (BCBS, 2022: 3). Operasyonel risk türleri 4 grup altında izlenebilir: personel riski, sistem riski, süreç riski ve dış riskler.

Personel riski, banka yönetimi ve personelinin yetersizliği, ihmali, görevlerini bilmemeleri, kötüye kullanmaları veya suç sayılan fiillere kasten girişmeleri sonucunda ortaya çıkan risklerdir (Leblebici Teker, 2006). Personelin bilgi veya tecrübesinin yetersiz olması, motivasyon eksikliği, iş yükünün fazla olması, yerlerin düzensiz değişmesi, işyerinin uygun olmaması veya işyerindeki düzenin olmaması gibi unsurlar personel riskleri olarak sıralanabilir.

Sistem riski, bilgisayar ve iletişim sistemlerindeki teknik sorunlar ve arızalar, virüs sorunları, yetersiz veya güncel olmayan sistemlerden kaynaklanan sorunlar nedeniyle ortaya çıkan risklerdir. Yazılım ve donanım arızaları veya bilgisayar sistemlerinin müşterilerin taleplerini karşılayamaması sonucu ortaya çıkan veri, zaman ve finansal kayıplar sistem ve teknoloji risklerine örnek olarak verilebilir.

Süreç riski, banka faaliyetlerine ilişkin süreçlere veya süreçleri tamamlama işlevine sahip iç kontrollere ilişkin prosedürlerin bulunmaması veya mevcut prosedürlerin yanlış planlanması veya hatalı uygulanmasından kaynaklanan risklerdir. İş birimleri arasındaki bilgi akışındaki yetersizlikler, yetkilere ilişkin mekanizmaların bulunmaması, kurumun taşıdığı risklerin belirlenememesi ve risklerin çalışanlara yeterince bildirilmemesi bu tür risklere neden olan faktörler arasındadır (Can, 2003: 5).

Dış riskler, yalnızca dış etkenlerden kaynaklanan ve banka ile herhangi bir bağlantısı olmayan risklerdir (Babuşcu, 2005). Dış etkenlerden kaynaklanan bu risklere örnek olarak bankaya yönelik soygun girişimleri, dolandırıcılık girişimleri, terör eylemleri, doğal afetler, savaşlar sayılabilir.

4.3.2. Uyum Riskinin Operasyonel Süreçler İçerisindeki Yeri ve Proaktif Uygulamalar

Bankalarda operasyonel risk ve uyum fonksiyonları, düzenleyici otoritelerin verdiği para cezalardan kaçınılmasının sağlanmasında önemli bir rol oynamalıdır. Her iki fonksiyonun rolleri ve sorumlulukları genellikle birbiriyle örtüşmektedir. İç kontrol ve risk yönetimi faaliyetleri arasındaki ilişkinin sonuçlarından biri de operasyonel risk ve uyum riski olmak üzere iki tür riske dayanmaktadır (Zoet, v.d.: 159).

Çeşitli mevzuat ve düzenlemeler, bankaların uyum ve operasyonel risklerini yönetmeleri konusunda yükümlülükler getirmektedir. Örneğin, Basel Bankacılık Denetim Komitesi (BCBS), her bankanın uyum riski yönetimi için kendi risk yönetimi stratejisi ile tutarlı bir şekilde öncelikler belirlemesini ve uyum fonksiyonunu düzenlemesini şart koşmaktadır (BCBS, 2005: 8). Ayrıca BCBS uyum riski ile operasyonel riskin belirli yönleri arasında yakın ilişki bulunduğu için bazı bankaların uyum fonksiyonlarını operasyonel risk fonksiyonları altında düzenlemek isteyeceğini, bazı bankaların ise bu iki fonksiyon arasında bir mekanizma kurarak ayrı olarak yönetebileceğini belirtmiştir (BCBS, 2005: 8).

Bankanın operasyonel süreçleri içinde uyum riski yönetimi, bankacılık işlemlerinin mevzuata uygunluğunun sağlanmasında önemli bir rol oynar. Uyum riski, operasyonel süreçlerin etkinliğini ve verimliliğini olumsuz yönde etkileyebilir ya da kurumların hedeflerine ulaşmasını engelleyebilir. Örneğin, bir bankanın müşterilerinin kimlik bilgilerini doğru bir şekilde doğrulamaması, mevzuata uygun olmayan bir şekilde faiz oranları belirlemesi veya kredi verirken gereken kriterleri yerine getirmemesi uyum riskine neden olmaktadır. Bunun sonucunda da müşterilerin güvenini kaybetmesine ve finansal kayıplara neden olabilir.

Uyum riskini etkin bir şekilde yönetmek için proaktif uygulamaları benimsemek önemlidir. Banka uyum riskine maruz kalmamak için operasyonel risklerini çeşitli uygulamalar ile yönetebilmektedir. Bu uygulamaları şu şekilde sıralayabiliriz:

i. Uyum Kültürü Oluşturmak

Uyum kültürü, yasalara, düzenlemelere ve politikalara uyuma öncelik veren bir dizi paylaşılan değerdir. Bankalar, çalışanları uyumluluk gereklilikleri konusunda eğiterek ve çalışanları olası ihlalleri bildirmeye teşvik ederek bir uyum kültürü geliştirmelidir. Çalışanlar uyumluluğun önemini ve uyumsuzluğun sonuçlarını anladıklarında, düzenlemelere uyma olasılıkları daha yüksektir.

ii. Düzenli olarak riskleri değerlendirmek

Risk değerlendirmesi, potansiyel riskleri belirleme ve olasılıklarını ve etkilerini değerlendirme sürecidir. Banka uyum riskini etkin bir şekilde yönetebilmek için

operasyonlarındaki iş süreçlerini düzenli olarak gözden geçirmeli, değişen iş süreçlerindeki riskleri değerlendirmeli, operasyonlarındaki uyum riskine neden olabilecek riskleri belirlemeli ve yönetmelidir.

iii. Güçlü politika ve prosedürler oluşturmak

Bankacılık sektörü yasal otoriteler tarafından yoğun olarak düzenlenen bir sektör olduğu için bankanın uyması ve takip etmesi gereken mevzuatlar fazla sayıdadır. Bankalar bu mevzuatlara uyulması için de kendi içinde güçlü politika ve prosedürler oluşturarak çalışanlarına aktarabilmeli ve yeknesak iş uygulamalar geliştirmelidir. Politika ve prosedürler, bankaların çalışanların net ve tutarlı bir yaklaşıma sahip olmasını sağlamak için önemli bir araçtır. Uyum riski yönetiminde personel risklerinin en aza indirilebilmesi için de bu belgeler açık, öz, anlaşılır ve kolay erişilebilir olmalı ve sürekli güncel tutulmalıdır.

iv. Uyum süreçlerinde teknolojiden yararlanmak

Teknoloji, bankaların uyum süreçlerini kolaylaştırmasına, manuel hataları azaltmasına ve verimliliği artırmasına yardımcı olmaktadır. Otomasyon, insan hatası riskini azaltmaya ve çalışanların daha önemli görevlere odaklanması için zaman kazanmasına yardımcı olmaktadır. RegTech çözümleri ile bankaların uyum konularındaki izleme, risk değerlendirme ve raporlama faaliyetleri etkin şekilde yapılabilmekte ve uyum riski yönetimindeki operasyonel hatalar en aza indirilebilmektedir.

v. Düzenli eğitimler vermek

Çalışanlar, bir bankanın operasyonel hataya veya suistimale uğramasına neden olabilecek en önemli yapı taşıdır. Çalışanları hem teknik konularda eğitmek hem de etik konularda farkındalık sağlamak güçlü bir uyum kültürü oluşturmak için bir gerekliliktir. Böylece banka personeli kaynaklı operasyonel riskler nedeniyle bankanın maruz kalacağı uyum cezaları eğitim verilerek yönetilmiş olacaktır.

vi. İzleme ve denetim

Bankalar oluşturdukları mevzuatların etkinliğini, bunlara ne derecede uyulduğunu, operasyonel süreçlerdeki hata ve suistimalleri iç denetim aracılığıyla

izlemeli ve uyum riskinin yaratacağı kayıplar gerçekleşmeden aksiyon almalıdır. İç denetim birimleri RegTech çözümlerini kullanarak risk bazlı uzaktan denetimler ile anomalileri tespit edip hızlı aksiyon alabilir ve rutin işlemlerin denetiminde zaman kaybını önleyerek uyum riski yaratabilecek farklı alanlara yoğunlaşabilir.

Sonuç olarak yasal otoriteler tarafından düzenlenen mevzuatlar bankaların finansal yapılarının krizlere karşı sağlam olması, banka faaliyetlerinin sürdürülebilir olması ve müşterilere karşı yeknesak uygulamaların olması amacıyla geçmişte çıkarılan derslere dayanılarak çıkarılmaktadır. Bu amaçlara ulaşabilmek için bankaların organizasyonlarında sağlam bir uyum kültürü oluşturması hem kendi hem de bankacılık ve finansal sisteminin sağlamlığı açısından önemli bir araçtır. Bankalar bu kültürü oluşturmak ve devamını sağlamak için IIA'in üçlü hat sistemini benimsemeli, etkinliğini sağlamalı, sürekli geliştirmeli ve sektördeki gelişmelere ayak uydurmalıdır.

4.3.3. Wells Fargo Vakası

Amerika'nın en büyük bankalarından biri olan Wells Fargo, uyguladığı satış politikası nedeniyle uyum riski ortaya çıkmış ve çeşitli otoriteler tarafından para cezasına çarptırılmıştır. Bu vakanın seçilmesinin nedeni bankanın her iş sürecinin uyum riskine sebebiyet verebileceğini göstermesi ve tüketicinin korunması konusunda kesilen en büyük cezaya sahip olmasıdır.

4.3.3.1.Bankanın Kısa Tarihi

Wells Fargo Bankası Mart 1852'de Henry Wells ve William Fargo tarafından kurulmuştur. İlk ofisi California, San Francisco'da açılan ve kısa süre sonra diğer şehirlere yayılan banka, Amerika Birleşik Devletleri'nin batı kısmında altın alımı, poliçe satışı ve değerli eşyaların teslimi alanlarında faaliyet göstermektedir (Wells Fargo, t.y.).

1920'ler boyunca Wells Fargo, Batı ABD'de tarım, otomobil, havacılık ve film endüstrilerinin geliştirilmesinde kilit bir rol oynamış olup 1980'lerden itibaren bir dizi birleşme gerçekleştirmiştir. En dikkate değer olanı ise Banka'nın operasyonlarını ülke genelinde genişletmesine olanak tanıyan 2018 yılındaki Wachovia ile birleşmedir.

Banka günümüzde ticari bankacılık, yatırım bankacılığı, emeklilik hizmetleri ve hazine yönetimi gibi birçok alanda dünyanın önde gelen finans firmalarından biridir. Dünya çapında 8.600'den fazla lokasyonda yaklaşık 269.000 ekip üyesi ile faaliyet göstermekte olan banka, Fortune dergisi 2022 yılı Amerika'nın en büyük firmaları sıralamasında 41. sırada yer almaktadır (Wells Fargo, 2022).

4.3.3.2.Banka Satış Politikası

Pazarlamanın en etkili yöntemlerinden biri olan çapraz satış (cross selling), bankaların mevcut bir müşteriye sattıklarından farklı bir ürün veya hizmet satması; ek satış (upselling) ise bankaların müşterilere ihtiyaçlarını karşılamak için üst düzey ürünler satmasıdır (Hayes, 2022). Çapraz satışın amacı, satış faaliyetlerini mevcut bir müşteri tabanına yatay ve/veya dikey olarak çeşitlendirmektir (Büchner ve Mulvenna, 1998: 59). Eğer müşteriler bankaya katılırsa ve daha fazla ürün eklemeye ikna edilebilirlerse, bu onların gelecekte daha da fazla ürün ekleme şanslarını artırmaktadır (Tayan, 2019). Tayan, daha fazla ürüne sahip müşterilerin banka için daha karlı olduğunu, hatta beş ürünü olan bir müşterinin üç ürünü olan bir müşteriden üç kat daha karlı olduğunu belirtmiştir.

2003 yılında Wells Fargo, satışların yılın ilk ayında güçlü bir şekilde başlamasına yardımcı olmak için "Ocak ayına atla (Jump into January)" satış kampanyasını oluşturmuştur. Bu kampanya ile Ocak ayında günlük satış hedefleri daha yüksek belirlenmiş, yönetim bu yüksek hedefleri vurgulamış ve bu hedeflere ulaşan çalışanları ödüllendirmiştir (SEC, 2017: 21).

2009 yılında Banka, rakiplerinden farklılaşmak için yeni bir satış programı geliştirmiştir. Ana hedef, mevcut müşterilere bankacılık ürün ve hizmetlerinin çapraz satışında pazar lideri olmaktır. Banka, her müşteri için kendisiyle en az sekiz ürünü olması için bir hedef belirlemiştir. Ek ürün satışları ile banka her müşteri hakkında daha fazla bilgiye sahip olmayı ve müşterilerin bankadaki işlem hacimlerini artırmayı hedeflemiştir (Witman, 2018: 133).

Wells Fargo üst yönetimi, satış hedeflerinden genellikle "50/50 planları" olarak söz etmesinin nedeni bölgelerin yalnızca yaklaşık yarısının hedefi karşılayabileceğini bilmesidir (SEC, 2017: 19). Fakat yönetim bu sayıları karşılamanın veya aşmanın

kariyerlerini iyileştirebileceğini veya bozabileceğini çalışanlar tarafından bilinmesini ve çalışanların satış hedeflerinin baskısını hissetmesini istemiştir. 2014 yılına kadar, çalışanlar ve yöneticiler günlük ve/veya haftalık bir "motivasyon raporu" almışlardır. Bu rapor aylık, üç aylık ve yılbaşından bugüne satış hedeflerini içermekte ve ayrıca çalışanları ve yöneticileri satış sonuçları açısından birbirlerine göre sıralanmaktadır (SEC, 2017: 20).

4.3.3.3. Skandalın Gelişimi

Satış baskısının yüksek olduğu bu tür bir iş modeli altında yönetim, gerçekçi olmayan satış kotaları uygulayabilmiş ve çalışanlarını bu ulaşılamaz hedeflere ulaşmak için hileli davranışlarda bulunmaya iten politikalar benimsemiştir. Satış hedeflerine ulaşmak ve ek tazminat kazanmak için çalışanlar, müşterilerin haberleri olmadan kredi kartı ve mevduat hesabı açmak için müşteri bilgilerini kullanmıştır. Bu çalışanların hedef müşterileri, bankacılık ilişkilerinde herhangi bir tutarsızlık fark etmeyeceklerini düşündükleri yaşlı ya da dil yeteneği iyi olmayan müşteriler gibi müşterilerdir (Elson ve Ingram, 2018: 127). Bazı şubelerde Wells Fargo çalışanları rutin olarak gündelikçilerin uğrak yerlerine gittiklerini ve banka şubesine gelip hesap açmak için her birine küçük bir meblağ ödediklerini bildirmiştir (Payne, 2017). İşçiler genellikle çok az İngilizce konuşmakta ve ne için kaydolduklarını anlamamaktadır. Birçok durumda bu, işçileri bankaya karşı aylık veya yıllık ücretlere ve diğer yükümlülüklere maruz bırakmıştır (Witman 2018: 132).

Satış hedeflerini gerçekleştiren çalışanlar ve yönetim, Banka'nın teşvik edici ücretlendirme programı kapsamında finansal ödüller kazanmıştır. Performans ölçüsü satış hacmi olduğu için üst yönetim günlük satışları artırmaya teşvik etmiş ve şube personeline yıllar içinde artarak devam eden satış hedefleri belirlemiştir.

Banka personelleri satış hedeflerini tutturabilmek için yeni banka hesapları açmak amacıyla müşterilere sahte işler öne sürmüşler, müşterilere çek hesabının kredi kartıyla birlikte verildiğini söylemek gibi yanıltıcı satış konuşmaları yapmışlar, sahte e-posta için iletişim bilgileri alanlarına yanlış veriler girmişlerdir (Elson ve Ingram, 2018: 127). Bazı durumlarda, bir müşteriyi çevrimiçi bankacılık hizmetlerine kaydetmek için "noname@wellsfargo.com" e-posta adresini kullandıkları bildirilmiştir (Egan, 2017). İstenmeyen hesapların açılması nedeniyle de müşteriler

için beklenmeyen sonuçlar meydana gelmiş, örneğin sık sık kredi kartı başvurusu yapılması ve sorgulanması, açılan hesaplara ücret tahakkuk etmesi ve bunların ödenmemesi müşterilerin kredi puanlarını etkilemiştir (Myfico, t.y.).

Birçok Wells Fargo personeli, günlük kotaları karşılama çabasıyla genellikle arkadaşları veya aile üyeleri adına hesaplar açmıştır. Daha önce belirtildiği gibi, herhangi bir ücret olmadığı sürece, boş hesapların hesap sahibi üzerinde genellikle çok az doğrudan ve ani etkisi olmuştur. Kurulun soruşturma raporunda aktarılan bir örnek buna örnek olarak gösterilebilir: "Bir şube müdürünün 24 hesabı olan genç bir kızı, 18 hesabı olan yetişkin bir kızı, 21 hesabı olan bir kocası, 14 hesabı olan bir erkek kardeşi ve 4 hesabı olan bir babası bulunmaktadır" (SEC, 2017: 36).

Bazı personeller Banka'nın satış uygulamalarından rahatsız olduğu için endişelerini yönetime, Banka etik danışma hattına ve hatta genel müdüre bildirmiştir. Fakat bu bildirimler olumlu karşılanmamış ve bu personeller istifaya zorlanmış ya da işine son verilmiştir (Elson ve Ingram, 2018: 127).

2015 yılında Banka yetkisiz hesaplar ile ilgili bir sorunu olduğunu kabul etmiş ve iç soruşturma başlatmıştır. Konu yerel savcılığın, Tüketici Finansal Koruma Bürosu'nun (CFPB - Consumer Financial Protection Bureau) ve federal yetkililerin dikkatini çekmiş ve Bankaya 185 milyon $ para cezası verilmiştir. 2011-2015 yılları arasında müşterilerin bilgisi veya izni olmaksızın iki milyonu aşkın kredi kartı ve banka hesabı açıldığı iddiası birçok denetim organının da dikkatini çekmiş ve ayrı soruşturmalar başlatılmıştır (Elson ve Ingram, 2018: 128).

Skandal 2016 yılında kamuoyuna duyurulduğunda Wells Fargo, 5.300'den fazla çalışanın kurumsal etik kurallarına (özellikle müşteri rızası gerekliliklerine) uymadığı için işine son verildiğini bildirmiştir. Belirlemelerin sadece dokuzu şube müdürü seviyesinin üzerindeki yönetim kadrosu içindir (Witman 2018: 134).

Banka, Eylül 2016'da satış programını 1 Ocak 2017 tarihinden itibaren sonlandıracağını ve müşteri hizmetleri, büyüme ve risk yönetimi odaklı yeni bir performans planına geçeceğini duyurmuştur. Tablo 4.3'te eski ve yeni performans planları karşılaştırılması gösterilmiştir.

Tablo 4.3 : Wells Fargo Teşvik Planları Karşılaştırması

Önceki Teşvik Planı	2017 Teşvik Planı
Çalışanlar teşvik almak için ürün satış hedefi minimumlarına ulaşmalıdır	Ürün satış hedefi yoktur
Müşteri kullanımına bakılmaksızın bankacıya anında ürün satış kredisi sağlanmaktadır	Teşvikler, müşteri hizmetlerine, şube birincil müşteri büyümesine (yani, ana finans kurumu olarak Wells Fargo'yu kullanan çek hesabı müşterilerinin büyümesine) dayalıdır
Çoğu satış ölçütü bireysel ve nicel tabanlıdır	Giriş seviyesi bankacı teşvik ödeme planları, takım performansına karşı bireysel performansa dayalıdır
Yerel yönetime dayalı birincil gözetim bulunmaktadır	Gizli müşteri ve şikayetler yoluyla faaliyetler yerinde izlenir; yerel, bölgesel ve kurumsal gözetim bulunmaktadır

Kaynak: Wells Fargo, 2017

Ocak 2017'de Wells Fargo, belirli satış kotalarını ortadan kaldıran yeni ölçümlerini ve teşvik programını duyurmuştur. Teşvikler aynı zamanda müşteri memnuniyetine de odaklanmakta, daha ekip bazlı olmakta (en azından giriş seviyesindeki personel için) ve uygun davranışı sağlamak için daha çok bir gözetim işlevi taşımaktadır. Wells Fargo, bu yeni teşvik programının, skandalı hızlandıran kötü davranışları caydırırken doğru davranışları teşvik edeceğini ümit etmiştir (Witman 2018: 136).

Denetimlerini sürdüren muhasebe firması, 2011-2015 yılları arasında yaklaşık 565 bin kredi kartı hesabının ve 1,5 milyon mevduat hesabının müşterilerin onayı olmadan açıldığını tespit etmiştir. Ağustos 2017'de Banka'nın yaptığı genişletilmiş incelemede ise, müşterilerin yetkilendirmemiş olabileceği toplam 3,5 milyon hesap ve müşterilerin bilgileri veya rızaları olmadan otomatik ödeme talimatı verilen 528.000 vaka tespit edilmiştir. Banka, bu hizmet için ücret veya başka masraflara maruz kalan müşterilere yaklaşık 1 milyon $'ı iade etmeyi kabul etmiştir (Elson ve Ingram, 2018: 128).

Satış hedeflerini tutturamayan ve/veya yöneticilerini Banka etik hattına bildirdikleri için kariyerleri etkilenen yaklaşık 500 çalışan, Banka aleyhine kendi davalarını açarak tazminat almıştır. Ekim 2016'da CEO, muhasebe skandalından

kaynaklanan kamuoyu tepkisi nedeniyle 34 yıllık kariyerine son vererek Banka'dan erken emekli olmayı seçmiştir.

Aşağıdaki tabloda Banka'nın yıllar içinde sonuçlanan soruşturmalara göre yasal otoriteler tarafından verilen para cezaları gösterilmiştir. Ancak tabloda Banka'ya açılan hukuk davaları kapsamında verilen tazminatlar dahil edilmemiştir.

Tablo 4.4 : Wells Fargo'ya Verilen Para Cezaları

Tarih	Ceza Tutarı	Yasal Otorite
Eylül 2016	185 Milyon $	100 milyon $ CFPB Civil Penalty Fund 35 milyon $ OCC 50 milyon $ City of Los Angeles
Ekim 2018	65 Milyon $	New York Attorney General
Nisan 2018	1 Milyar $	OCC ve CFPB
Aralık 2018	575 Milyon $	50 Eyalet ve Kolombiya Bölgesi
Şubat 2020	3 Milyar $	500 milyon $ yatırımcılara dağıtılmak üzere SEC'e 2,5 milyar $ ABD Hazinesine
Eylül 2021	72,6 Milyon $	Justice Department
Aralık 2022	3,7 Milyar $	CFPB, "yasadışı faaliyet" nedeniyle 1,7 milyar $ para cezası ve 2 milyar $ tüketici tazmini ödemesi

Kaynak: Violation Tracker, 2023

Sonuç olarak Banka uyguladığı satış politikası nedeniyle personellerine satış baskısı kurarak operasyonel riske sebebiyet vermiş, operasyonel risklerini yönetememiş, iç kontrol ortamını sağlayamamış ve bunların neticesinde uyum riskine maruz kalarak 8,5 milyar $ para cezası ödemek zorunda kalmıştır.

4.3.3.4. Çıkarılacak Sonuçlar

Wells Fargo skandalı Banka yönetiminin, uyum görevlilerinin, iç ve dış denetçilerin uyum riski yönetimini etkili bir şekilde yönetemediğini ve bankanın çeşitli politikaları ile iç kontrol ortamı dengesinin kurulmasının önemini göstermiştir.

Wells Fargo bağımsız yönetim kurulu üyelerinin yayınladığı raporda;

- Bankanın kontrol fonksiyonlarına işlem odaklı ve dar açıdan baktığı, şikâyet ve bireysel davalara odaklandığı, bunları satış uygulaması sorunu olarak gördüğü ve sistematik bir sorun olduğunu tespit edemediği (SEC, 2017: 13),

- Operasyonel risk yetkilisinin satış uygulamalarını veya tazminat konularını kendi yetkisi dahilinde değil de diğer departmanların sorumluluğu olarak düşündüğü ve satışların iyi yönetilen, kontrol edilen ve küçük bir sorun olarak gördüğü (SEC, 2017: 61),
- Hukuk departmanının esas olarak ölçülebilir maliyetlere veya cezalara odaklandığı, bu maliyetlerin de küçük tutarlar olacağını düşündüğü ve satış sorunlarının sistematik bir sorun olarak görmediği (SEC, 2017: 78),
- İnsan kaynakları departmanının elinde birçok veri olduğu fakat satış uygulamaları konusunda bilgileri konsolide edecek ve raporlayacak araçları geliştirmedikleri (SEC, 2017: 79),
- İç denetim departmanının genel olarak satış uygulaması ihlallerini tespit etmek, araştırmak ve düzeltmek için tasarlanan süreç ve kontrollerin, satış uygulamalarıyla ilgili riskleri azaltmada etkili olduğunu tespit ettiği fakat departmanın etik olmayan satış uygulamalarının temel nedenini belirlemeye çalışmadığı (SEC, 2017: 91)

belirtilmiştir.

Sonuç olarak Wells Fargo'ya satış politikaları sebebiyle verilen uyum cezası, bankaların AML/CFT/KYC süreçlerinin yanında birçok faaliyeti için uyum risklerini değerlendirmeleri gerektiğini göstermiştir. Ayrıca risk yönetiminin süreç temelli yönetilmesi gerektiği, RegTech çözümleri gibi teknolojik altyapıları kullanan uygulamalar ile uyum risklerinin belirlenmesi ve yönetilmesinde etkinliğin sağlanması gerektiği ve ceza riskini önlemek için bankanın personellerinden üst düzey yöneticilerine kadar herkesi kapsayan bir uyum kültürü oluşturmanın önemli olduğu Wells Fargo'ya verilen ceza ile görülmüştür.

4.4. Bankacılıkta Uyum Riskine Yönelik RegTech Kullanım Alanları

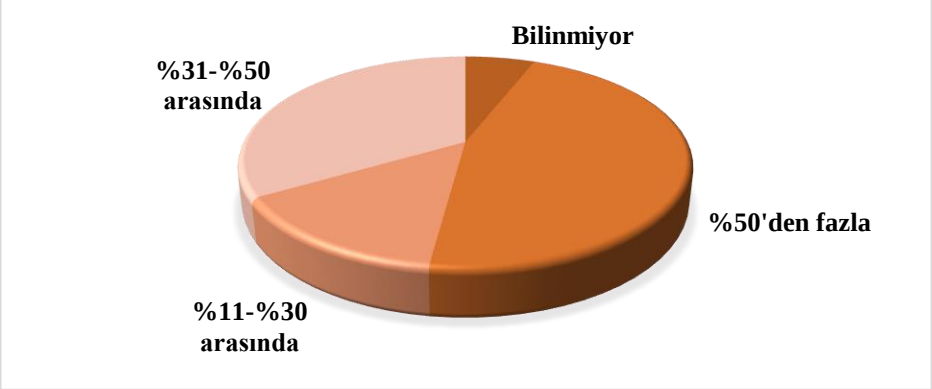
Uyum riskinin yönetilmesinde kullanılan RegTech çözümleri, Türkiye'de uyum konusu ve RegTech sektörü ile iç denetimde kullanım alanları örnekler verilerek aşağıdaki başlıklar altında incelenmiştir.

4.4.1. RegTech Kullanım Alanları ve Firma Örnekleri

RegTech firmaları mevzuata uyum, kimlik yönetimi ve kontrolü, risk yönetimi, yasal raporlama ve işlem izleme gibi birçok uyum konusunda finansal firmalara çözüm sunmaktadır. Farklı teknolojik yazılımlar kullanılarak firmaların zaman ve maliyet tasarrufu sağlamaları ve uyum riskini etkin yönetmeleri sağlanmaktadır.

Deloitte firmasının 2021 yılında yayınladığı rapordaki 117 RegTech uygulamasının ne kadar zaman ve maliyet tasarrufu sağladığı Grafik 4.5 ve Grafik 4.6'da gösterilmektedir.

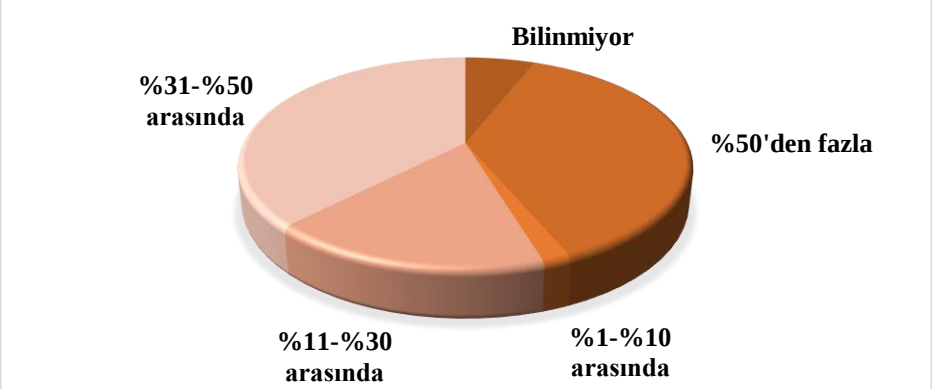
Grafik 4.5 : Deloitte Araştırmasındaki Uygulamaların Zaman Tasarrufu Sağlama Oranları



Kaynak: Deloitte, 2021

İlgili raporda 117 adet uygulamanın 54'ünün %50'den fazla, 39'unun %31 ila %50 arasında, 17'sinin ise %11 ila %30 arasında zaman tasarrufu sağladığı belirtilmiş olup 7 adet uygulamaya ait veri bulunmamaktadır (Deloitte, 2021).

Grafik 4.6 : Deloitte Araştırmasındaki Uygulamaların Maliyet Tasarrufu Sağlama Oranları

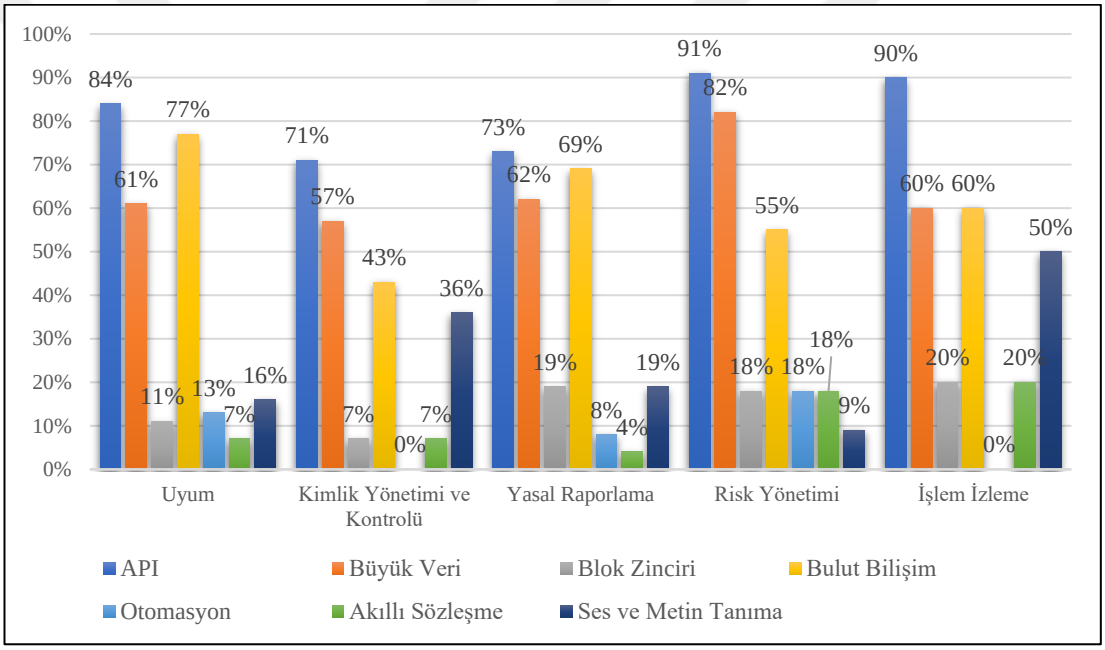


Kaynak: Deloitte, 2021

İlgili raporda 117 adet uygulamanın 44'ünün %50'den fazla, 44'ünün %31 ila %50 arasında, 20'sinin %11 ila %30 arasında, 2'sinin ise %1 ila %10 arasında maliyet tasarrufu sağladığı belirtilmiş olup 7 adet uygulamaya ait veri bulunmamaktadır (Deloitte, 2021).

RegTech uygulamalarının %79'unun %30 üzeri zaman tasarrufu ve %75'inin %30 üzeri maliyet tasarrufu sağlaması uyum riskinin etkin bir şekilde yönetilmesinde bu çözümlerin kullanılmasının önemli olduğunu göstermektedir.

Grafik 4.7 : Deloitte Araştırmasındaki Uygulamaların Kullandığı Teknolojilerin Alanlarına Göre Oranı



Kaynak: Deloitte, 2021

İlgili raporda RegTech uygulamalarının hangi alanda hizmet verdiği ve hangi teknolojileri kullandığı incelenmiştir. 117 adet RegTech uygulamasının 56'sının uyum, 26'sının yasal raporlama, 14'ünün kimlik yönetimi ve kontrolü, 11'inin risk yönetimi ve 10'unun işlem izleme alanlarında hizmet verdiği görülmüştür.

Raporda aynı uygulamada birden fazla farklı teknolojinin kullanıldığı görülmektedir. Kullanılan teknolojilere baktığımızda API teknolojisinin 95, büyük veri teknolojisinin 70, bulut bilişim teknolojisinin 67, ses ve metin tanıma teknolojisinin 19, blok zinciri teknolojisinin 13, otomasyon teknolojisinin 11 ve akıllı sözleşme teknolojisinin 9 uygulamada kullanıldığı tespit edilmiştir (Deloitte, 2021).

Grafik 4.7'de RegTech uygulamalarında kullanılan teknolojiler alanlarına göre gösterilmiştir. Hizmet alanlarındaki uygulama sayıları farklı olduğu için ilgili grafikte teknolojilerin kullanıldığı alan içindeki oranı gösterilmiştir. Grafiğe baktığımızda her alanda yüksek oranda API teknolojisinin kullanıldığı, uyum ve yasal raporlama alanlarında en fazla kullanılan ikinci teknolojinin bulut bilişim teknolojisi olduğu, kimlik yönetimi ve kontrolü ile risk yönetimi alanlarında en fazla kullanılan ikinci teknolojinin büyük veri teknolojisi olduğu, işlem izleme alanlarında ise bulut bilişim ve büyük veri teknolojilerinin eşit oranda kullanıldığı görülmektedir. API teknolojisinin her alanda yüksek oranda kullanılmasının nedeninin son yıllarda açık bankacılık alanında yaşanan gelişmeler ve açık bankacılık uygulamalarının yaygınlaşması olduğu söylenebilir.

FinTech Global, dünyanın önde gelen FinTech bilgi hizmetleri, B2B medya ürünleri ve endüstri etkinlikleri sağlayıcısıdır (Fintech Global, t.y.). Her yıl endüstri uzmanları ve analistlerden oluşan bir jüri tarafından seçilen dünyanın en yenilikçi 100 RegTech firmasını REGTECH100 adlı raporunda açıklamaktadır. Liste oluşturulurken sunulan çözümün endüstrideki önemi ve teknolojik yeniliği, firmanın topladığı sermaye ve elde ettiği gelir, ilgili çözümün müşteriler için potansiyel maliyet tasarrufu, verimlilik artışı ve/veya gelir artışı yaratıp yaratmadığı gibi kriterler dikkate alınmıştır (RegTech Analyst ve Fintech Global, 2022). 2023 yılında yayınlanan REGTECH100 raporundaki firmalara birkaç örnek verilebilir:

i. *Actico* firması 2015 yılında Almanya'da kurulmuştur. Firmanın sunduğu "ACTICO Compliance Suite" uygulaması riskleri yönetmek, AML/KYC/CDD gibi yasal uyumluluk yükümlülüklerini yerine getirmek, dolandırıcılığı önlemek, dijital müşteri etkileşimini geliştirmek ve operasyonları optimize etmek için kullanılmaktadır. Akıllı otomasyon ve dijital karar verme için tasarlanmış olan uygulama, insan bilgisi ile yapay zekayı otomasyon teknolojisiyle birleştirmektedir. İlgili yazılım Santander, Swiss Life, Bayerische Landesbank, ING, KfW Development Bank, LGT Bank, VP Bank Group, Maybank, UBS Hongkong gibi bankalarda kullanılmaktadır (RegTech Analyst ve Fintech Global, 2022: 11).

ii. *AML Partners* firması 2006 yılında Amerika'da kurulmuştur. Firmanın sunduğu "RegTechONE" uygulaması, uyum görevlilerinin kara para aklama ve terörün finansmanına karışan müşterileri en iyi şekilde belirlemek ve bunlarla ilgili işlem yapmak için GRC/AML yazılımları üzerinden çözüm sunmaktadır. İlgili yazılım Mashreq Bank, China Construction Bank, National Bank of Kuwait, United Bank for Africa gibi bankalarda kullanılmaktadır (RegTech Analyst ve Fintech Global, 2022: 15).

iii. *S&P Global Market Intelligence Cappitech* firmasının sunduğu "Cappitech" uygulaması yasal raporlama ve uyum yönetimi alanlarında en iyi uygulama ve iş zekâsı çözümleri sağlamaktadır. İlgili uygulama işlem raporlama alanındaki tüm raporların otomasyonunu sağlamakta ve Dünya'da 500'den fazla finansal kurumda kullanılmaktadır (RegTech Analyst ve Fintech Global, 2022: 30).

iv. *Know Your Customer* firması 2015 yılında kurulmuş olup Hong Kong, Singapur, İngiltere ve İrlanda'da ofisleri bulunmaktadır. Firmanın sunduğu çözümler, uyum ekiplerinin mali suç riskini azaltmasına, çevik otomasyon ve iş akışları yoluyla süreçleri kolaylaştırmasına, şirket kayıtlarına canlı bağlantılar sağlayarak veri doğruluğunu iyileştirmesine ve şirket içi, yönetim kurulu ve yasal otorite taleplerine daha verimli bir şekilde uymasına olanak tanımaktadır. Firma ürünlerinde KYC ve KYB süreçlerini tamamen dijitalleştirmek için yapay zekâ, makine öğrenimi, optik karakter tanıma (optical character recognition-OCR), doğal dil işleme (natural language processing-NLP) ve yüz tanıma teknolojilerini kullanır. Müşteri arasında Hamburg Commercial Bank gibi bankalar ve One4All, Premium Credit, ConnectPay, Crosscard gibi ödeme kuruluşları bulunmaktadır (RegTech Analyst ve Fintech Global, 2022: 84).

4.4.2. Türkiye Bankacılık Sistemine RegTech Çözümleri Entegrasyonu

FinTech sektörü ile karşılaştırıldığında RegTech sektörü globalde gelişime açık bir alan olarak görülmektedir. FinTech yatırımları 2021 yılında 7.321 anlaşmada 238,9 milyar $'lık rekor seviyeye ulaşmasına karşın RegTech yatırımları 2021 yılında 444 anlaşmada 18,9 milyar $ seviyesindedir (Bignell, 2023). REGnosys CEO'su Leo Labeis RegTech çözümlerinin sadece "olsa iyi olur" olarak görülmemesi gerektiğini,

RegTech'in düzenleyici kurumların giderek artan sayıda düzenlemelerine ve incelemelerine karşın finansal kurumların düzenlemelere uymasına yardımcı olduğunu ve RegTech'e yapılan harcamaların yalnızca 2026'da üçe katlanacağını belirtmiştir (Bignell, 2023). Juniper Research, RegTech sektörünün 2022-2026 arasında %200 büyüyeceğini (Fintech İstanbul, 2022b), Goode Intelligence ise "Identity Verification (IDV) Market & Technology Analysis & Forecasts 2021-2026" raporunda sadece uzaktan kimlik doğrulama pazarının 2026 yılına kadar 17 milyar $'ı aşarak yüzde 22 oranında büyüyeceğini ve 2021 yılındaki 1,1 milyar uzaktan kimlik doğrulama işlem sayısının 3 katına çıkarak 2026'da 3,8 milyar olacağını tahmin etmektedir (Fintech İstanbul, 2023).

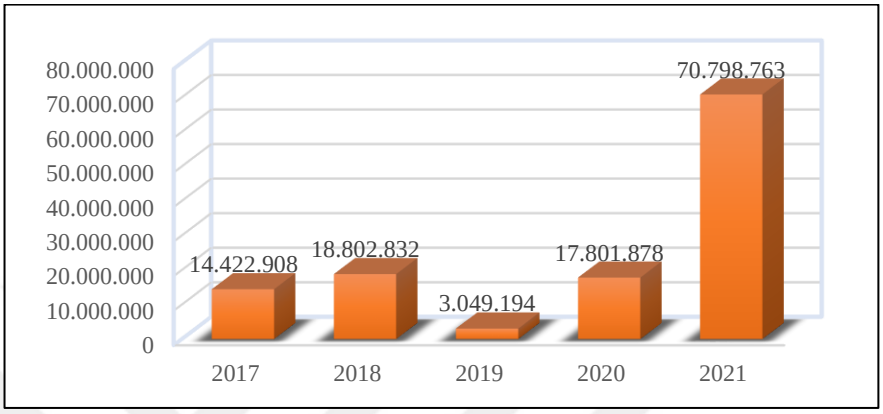
Türkiye'de ise RegTech ekosistemi henüz oluşum aşamasındadır. Uyum konusunda dijital ortamı destekleyen bir düzenleme olmadığından yatırımcılar için RegTech alanı hem bir fırsat hem de bir risk olarak görülmektedir. 2015 yılında yayımlanan Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ile FinTech firmalarının sayısının artması gibi RegTech'ler için de yapılacak bir düzenleme ekosistemin büyümesine katkı sağlayabilir (Uzunoğlu, E., t.y.).

2019 yılında kurulan kara para aklamayı önleme çözümleri sunan Sanction Scanner firması Türkiye'den bir RegTech firması olarak örnek gösterilebilir. 4 kıtada 40'tan fazla ülkede 2 uluslararası ofisiyle 300'den fazla müşteriye hizmet vermektedir (Sanction Scanner, t.y.(a)). Türkiye'nin en hızlı büyüyen teknoloji firmalarını ödüllendirdiği 2022 yılı Deloitte 17. Teknoloji Fast 50 töreninde ödül almış (Sanction Scanner, t.y.(b)) ve RegTech pazarında dünyanın önde gelen firmalarının listelendiği RegTech Analyst'in yayımladığı 2023 yılı 6. RegTech100 listesine girmiştir (Sanction Scanner, t.y.(c)).

FATF Küresel suç gelirlerinin aklanması ve terör finansmanı izleme kuruluşudur. Bir ülkenin FATF Gri Listesinde yer alması, o ülkenin belirlenen stratejik eksikliklerini, kararlaştırılan zaman dilimleri içinde hızlı bir şekilde çözmeyi taahhüt ettiğini ve ekstra kontrollere tabi tutulacağını göstermektedir. Türkiye 2019 yılında karşılıklı değerlendirmenin kabul edilmesi sonrası FATF tarafından takip sürecine alınmış, 2021 yılında ise FATF tavsiyelerine uyumu yeniden derecelendirilmiş ve Gri

Listeye alınmıştır (Sanction Scanner, 2022: 3). 24 Şubat 2023 tarihindeki genel kurulunda Türkiye'nin hala Gri Listede olduğu görülmektedir (FATF, 2023).

Grafik 4.8 :Türkiye'de İdari Para Cezasına Konu Fiillerin Yıllar İtibarıyla Grafiksel Dağılımı



Kaynak: MASAK, 2021: 36

Grafik 4.8'de MASAK'ın 2021 yılı faaliyet raporunda 2017-2021 yılları arasındaki toplam idari para cezalar belirtilmiştir. İlgili yıllar içerisinde 2019 yılında diğer yıllara göre daha az idari para cezası verildiği ve 2021 yılında bir önceki yıla göre neredeyse 3 kat arttığı görülmektedir. Bunun sebebi ise 2019 yılında 17, 2020 yılında 135, 2021 yılında ise 245 yükümlülüklere uyum denetimi yapılması yani yıllara göre değişen denetim sayıları gösterilebilir (MASAK, 2021: 35).

BDDK'nın 2021 yılı faaliyet raporu incelendiğinde;

- Kurul kararları içerisinde "idari para cezaları" konulu 2020 yılında 367 adet, 2021 yılında ise 362 adet karar olduğu ve bu kararların tüm kararlar içerisindeki oranlarının sırasıyla %60,5 ve %55,2 olduğu (BDDK, 2021: 19),
- 2021 yılı içerisinde bankalar hakkında 47 adet idari para cezası uyguladığı (BDDK, 2021: 54),
- Bilgi sistemleri değerlendirme ve uygulama faaliyetleri kapsamında, bilgi sistemlerine ilişkin mevzuata uyumsuzluk nedeniyle 4 adet mevduat ve katılım bankasına, 2 adet kalkınma ve yatırım bankasına idari para cezası uyguladığı (BDDK, 2021: 46),
- 2021 yılında bireysel nitelikte ürün ve hizmetlerle ilgili gelen ihbar, şikâyet, başvurular nedeniyle yapılan denetimler sonucunda 200 adet kurul kararıyla

toplamda bankalara 61.126.869 TL idari para cezası uygulandığı (BDDK, 2021: 59) belirtilmiştir.

Ayrıca basında çıkan idari para cezası konularındaki haberler incelendiğinde şu örnekler verilebilir:

i. 2020 yılı cezaları

BDDK tarafından "bankalara iletilen talimatlara aykırı işlem tesis edilmesi" gerekçesiyle 15 Mayıs 2020 tarihinde 15 bankaya toplamda 19 milyon 650 bin TL, 29 Mayıs 2020 tarihinde 18 bankaya toplam 102,1 milyon TL ve 9 Temmuz 2020 tarihinde "müşteri şikayetleri" ve "talimatlara aykırılık" gerekçesiyle 7 bankaya toplam 204 milyon 651 bin TL olmak üzere 2020 yılı içerisinde bankalara toplamda 326 milyon 401 bin TL idari para cezası verilmiştir (Sözcü, 2020).

ii. 2021 yılı cezaları

BDDK bankalara bireysel veya tüzel müşterilere Türk Lirası cinsinden kullandırılan kredilerin amacına aykırı işlemlere konu edilmemesine yönelik gerekli kontrollerin azami seviyede oluşturulması uyarısında bulunmuş ve Bankacılık Kanunu'nun 148. maddenin b fıkrasındaki hüküm gereğince bu düzenlemeye uymayan 13 Bankaya 50'şer bin TL idari para cezası vermiştir.

iii. 2023 yılı cezaları

TCMB, Aralık ayında Bankalara gönderilen yazıda "ödemeler alanında şeffaflığı arttırmak amacıyla ödeme kategorisi detayı gibi bazı alanları eksik raporlayan, hatalı raporlama yapan ve/veya TL ve yabancı para ödemeleri gerekli belgelerle tevsik edemeyen (ithalat ödemesinde ilgili ithalat belgesinin sunulmaması, kredi ödemesi, menkul kıymet işlemleri gibi) bankalardan 2 Ocak 2023 tarihi itibarıyla tespite konu ödemenin yüzde 5'i kadar ek ücret alınacağını" belirtmiştir (Bloomberght, 2022). 2023 yılının Şubat ayında ise bankalara yurt dışına yapılan spot Döviz transferlerinde bilgilendirme yükümlülüğünü yerine getirmedikleri gerekçesiyle "ceza niteliğinde" toplamda 700 milyon TL'ye yakın ek ücret uyguladığı, bu uygulamalardan en büyük olanların 240 milyon TL ile Akbank'ta olduğu, Yapı Kredi Bankası'na

150 milyon TL, Garanti Bankası'na 120 milyon TL, Denizbank'a 100 milyon TL ve İş Bankası'na ise 50 milyon TL ek ücret uygulandığı belirtilmiştir (Bloomberght, 2023a).

4.4.3. Halkbank Vakası

2012 yılında, İran'ın ana devlet petrol kuruluşu Ulusal İran Petrol Şirketi'nin (NIOC) Halkbank'ta mevduat hesapları bulunduğu bilinmektedir. ABD'nin İran yaptırımları, Türkiye'nin İran petrol ve gazını Türk lirası kullanarak satın almasına izin vermiş ancak İran'ın Halkbank nezdinde bulunan fonları farklı yerlerde kullanılması yasaklanmıştır (Scott, 2019: 735). Ayrıca 2012 ve 2013 yıllarında İran'a altın ve değerli metal ihracatı henüz yaptırımlarla yasaklanmamıştır. 2012 yılının Haziran ve Temmuz aylarında Türkiye'nin İran'a yaptığı aylık altın satışları 1,6 milyar $ ile zirve yapmıştır (Clark v.d., 2013: 1).

Reza Zarrab, Türk-İran asıllı, Türkiye, Dubai ve İran'da döviz ticareti ağına sahip olan bir iş adamıdır. Zarrab, İran yaptırımlarındaki açıkları hedef alarak çeşitli yöntemler geliştirmiş, Halkbank'taki NIOC hesaplarından İran Hükümeti adına Dubai'deki altın ve döviz borsalarına ve oradan çeşitli uluslararası noktalara para taşımak için kendi kontrolünde olan bir firmayı kullanmış ve yaptırım konularında uzman kişilerden yardım almıştır (Scott, 2019: 735).

Zarrab, 2016 yılında ailesiyle birlikte tatil için gittiği ABD'de tutuklanmış, kara para aklama, dolandırıcılık ve yaptırım ihlalleriyle suçlanmış, daha sonra Halkbank Genel Müdür Yardımcısı Hakan Atilla aleyhine ifade vermiştir. 2017 yılında ise Atilla tutuklanmış ve dolandırıcılık yapmak, kara para aklamak ABD makamları tarafından yaptırımları ihlal etmekle suçlanmıştır. Atilla, daha sonra 2018 yılında bazı suçlamalardan suçlu bulunarak 32 ay hapis cezasına çarptırılmıştır (Aljazeera, 2018). Güncel durumda 17 Şubat 2021'de ABD'de banka aleyhine açılan tazminat talepli hukuk davasının, 2 Mayıs 2023'te banka lehine karar verilerek düşürüldüğü, bununla birlikte, ABD Yüksek Mahkemesinin 19 Nisan 2023 tarihli kararı doğrultusunda ceza davası ile ilgili hukuki sürecin İkinci İstinaf Mahkemesi nezdinde devam ettiği görülmüştür (Bloomberght, 2023b).

4.4.3.1. Altın ve Gıda Yöntemi

Zarrab, yaptırımları aşmak için altın yöntemi ve gıda yöntemini kullanmıştır. Altın yöntemi yaptırımlarda yasal boşluk bulunduğu ve altının yüksek değerinden dolayı transferi kolay olduğu için kullanılmıştır. İran Halkbank nezdinde bulunan NIOC'e ait hesaplarında sadece TL olarak yararlanabilmiştir. Bunu aşmak için Türkiye ve Dubai'de iş ağına sahip olan Zarrab tarafından, Türk petrol rafineri firmasından Halkbank'taki NIOC hesaplarına para transferi aktarıldıktan sonra bunlar altın satın almak için kullanılmış, elde edilen altın Dubai'ye ihraç edilmiş ve altın nakde çevrildikten sonra da İran'ın kullanımı için uluslararası olarak çeşitli yerlere havale edilmiştir (U.S. District Court-Southern District of New York, 2017: 16-17).

2013 yılında altın da yaptırımlara dahil edilince altın yöntemine benzer şekilde gıda yöntemi kullanılmaya başlanmıştır. Bu yöntemde fonlar Halkbank'taki NIOC hesaplarından Zarrab tarafından kontrol edilen hesaplara taşınmış ancak yaptırım kısıtlamalarından muaf tutulan gıda ve ilaç ihracatına ilişkin fon transferlerinin kanıtlanması gerekmiştir. Bu da Dubai'den İran'a gıda ve ilaç sevkiyatını gösteren belgelerin oluşturulması gerektiği anlamına gelmektedir (U.S. District Court-Southern District of New York, 2017: 26). Zarrab verdiği ifadede hiçbir zaman İran'a yiyecek gönderilmediğini, bütün bunların talimat verilen uluslararası ödemeleri yapabilmek için geliştirilmiş bir sistem olduğunu ve amacın Halkbank'ta birikmiş olan parayı çıkarmak olduğunu belirtmiştir (U.S. District Court-Southern District of New York, 2018).

4.4.3.2. Uyum ve Risk Değerlendirmesi

Halkbank davası bankacılıkta KYC süreçlerinin ve uyum riski yönetiminin önemini göstermektedir. Politik bağlantıları bulunan, yüksek riskli ticari faaliyetler gerçekleştiren Reza Zarrab gibi müşteriler ile İran dışında tutulan ve yaptırım kısıtlamalarına tabi olan İran Hükümeti fonlarını içeren NIOC gibi firmalar, yüksek riskli kategorisine alınmalı ve işlemleri mümkün olan en katı kontroller ile kontrol edilmelidir.

Türkiye ile İran arasındaki doğrudan banka havalelerine dayalı izleme faaliyetleri bu tip ilişkileri ve mevzuata uygun olup olmadığını tespit edemeyecektir ancak NIOC gibi yüksek riskli müşterilere odaklanan ve hesap etkinliğindeki

açıklanamayan değişiklikleri gösterge olarak kullanan RegTech yazılımları, bu karmaşıklıktaki şemaları tespit etmenin en etkili yöntemi olabilir. Faaliyet tespit edildikten ve yasal otoritelere raporlandıktan sonra banka yükümlülüklerini yerine getirmiş olur. Gelecekte ilgili düzenlemeler yapıldıktan sonra AML ve KYC/KYB alanlarında faaliyet gösteren RegTech firmaları açık bankacılıkta yapıldığı gibi API'ler üzerinden global olarak işlem bilgilerini birbirleri ile paylaşabilir ve böylece yasal mevzuata uygun olmayan faaliyetler daha kolay tespit edilebilir.

Yasal otoriteler tarafından bankalara verilen cezaların finansal riskleri yanında itibari riski de bulunmaktadır. Banka üst düzey yöneticisinin gözaltına alınması ve mahkûm edilmesi, bankaya açılan davanın yıllar sürmesi ve basında çıkan haberler bankanın itibarını ve bankaya duyulan güveni zedelemiştir.

4.4.4. İç Denetimde RegTech Kullanım Alanları

Uyum riskinin yönetilmesi ve uyumsuzlukların tespit edilmesi hususunda birinci ve ikinci savunma hattının yanında üçüncü savunma hattı olan iç denetimin de rolü büyüktür. Geçmiş yıllar ile karşılaştırdığımızda veri yoğun bir sektör olan finans sektöründe her yıl daha fazla veri üretilmekte ve sektör büyümektedir. Dünyadaki tüm verilerin %90'ı sadece 2016-2018 yılları arasında üretilmiştir (Marr, 2018). Üretilen verinin geçen her zamanda katlanarak artması yapılan denetimlerde teknoloji ihtiyacını da artırmaktadır.

Günümüzde denetim anlayışı geleneksel denetimden risk bazlı, proaktif ve sürekli denetim anlayışına geçmiştir. Bu amaçla denetim teknolojilerinin kullanılması hem zamandan tasarruf sağlayacak hem de denetçilerin daha doğru analiz yapmalarına yardımcı olacaktır. Teknolojinin kullanılması denetçilerin işlerini kaybedecekleri anlamına gelmemeli sadece denetçinin muhakeme yeteneğini kullanması için yardımcı araç olarak görülmelidir (Zhu, 2021: 745). Hatta denetim teknolojilerine hâkim, bunları kullanabilen ve elde edilen veriyi analiz edebilen denetçi ihtiyacı bu teknolojilerin kullanımının yaygınlaşmasıyla birlikte artacaktır. Bir araştırmada bankaların büyük veri teknolojisine yatırım yaptıkları ve bu alanda uzman, veri analizi yeteneği kuvvetli ve bu veri analiz uygulamalarında yetkinlik sahibi çalışanlar talep ettikleri belirtilmiştir (Kara, v.d., 2019: 8).

Bankaların iç denetim birimi denetimlerini yerinden, uzaktan ve merkezden denetim faaliyetleri olarak yapmaktadır. Uzaktan denetim, denetçinin iç kontrol sistemini değerlendirdiği, kanıt toplama, analiz yapma ve raporlama gibi süreçlerde çeşitli teknolojilerden yararlandığı ve denetlediği birimde fiziken bulunmadığı bir denetim türüdür (Teeter v.d., 2010: 74). Merkezden denetim ise bankacılık işlemleri üzerinden çeşitli risklere göre senaryoların kurgulandığı, bu kurgunun çeşitli analitik araçlar ile formül haline getirildiği ve bu senaryoya uyan tespitlerin sürekli olarak denetlendiği ve analiz edildiği denetim türüdür.

Uzaktan ve merkezden denetim faaliyetlerinde kullanılan veri madenciliği, büyük veri ve veri analitik araçları, risk yönetimi ve robotik süreç otomasyon yazılımları gibi teknolojiler aslında birer RegTech çözümleridir. RegTech 3.0 ile gelen yapay zekâ, dağıtık defter teknolojisi, API gibi teknolojileri kullanan uygulamalar denetim alanında yaygın olmasa da denetimin kalitesini, etkinliğini ve verimliliğini artırmak amacıyla ileriki zamanlarda yaygın şekilde kullanılacaktır. Uzaktan denetim ve yerinde denetim birbirinin ikamesi değil tamamlayıcısı (Gürkan, 2021: 33) olsa da RegTech uygulamalarının kullanılması ile birlikte uzaktan denetimin payı artacak ve risk bazlı sürekli denetimler geleneksel denetimin yerini alacaktır.

Denetim alanında kullanılabilecek RegTech uygulamalarına örnek vermek gerekirse; Mindbridge, finansal işlemlerin şeffaflığını ve bütünlüğünü sağlayarak kuruluşların finansal kayıplarını en aza indirmelerine yardımcı olmak amacıyla 2015 yılında Kanada'da kurulan RegTech firmasıdır (CBinsights, t.y.). Firmanın sunduğu uygulama finans uzmanları ve denetçiler için tasarlanmış, makine öğrenimi ve yapay zeka tekniklerini kullanarak verilerin hepsinin risk seviyesini çeşitli kontrol noktalarına göre belirleyen ve anomalileri tespit eden bir uygulamadır (Mindbridge, t.y.). Uygulamanın çok kısa sürede büyük verileri analiz etmesi denetçinin çeşitli suistimal, dolandırıcılık ve hataları tespit etmesine yardımcı olacaktır. Firmanın CEO'su Eli Fathi, yapay zekânın kullanımının her büyüklükteki firmanın denetim kalitesini ve risk güvencesini artıracağını savunmaktadır (Williams, 2018).

SONUÇ

Ülke ekonomilerinin yapı taşları olan finansal kurumlar arasında bulunan bankalar ekonomik krizlerden ciddi zarar gören taraf olmuştur. Türkiye'de yaşanan 2001 krizi ve globaldeki 2008 krizi, krizleri önlemek için yapılması gereken düzenlemelerin önemini ortaya çıkarmıştır. Sektörün krizlere karşı sağlamlaştırılması adına dünyada kabul gören Basel düzenlemeleri ile bölgesel ve yerel yasal otoriteler tarafından yapılan düzenlemeler yıldan yıla artmış ve bankaların bu düzenlemelere uyması beklenmiştir.

Bankalar yasal otoritelerin getirdiği düzenlemelere uymaması durumlarında çeşitli yaptırımlara maruz kalabilmektedir. Bu yaptırımlar uyumsuzluğu düzeyine bağlıdır. Uzun süre yapılan ve yüksek tutarlı olan uyumsuzluk sonucunda bankanın işlemlerinin incelenmesi, soruşturulması ve uzun süre gündemde tutulduktan sonra para cezası verilmesi hem bankanın mali yapısını hem bankanın borsadaki hisse senedi değerindeki düşüş nedeniyle yatırımcısını hem de güven kaybı ile itibarını zedelemektedir.

Bankalarda potansiyel zarar kayıplarının önlenmesi için uyum riski yönetiminde kullandıkları çeşitli araçlar vardır. Bu araçlar RegTech çözümleridir. Bankacılıkta bilgisayarın yaygınlaştığı RegTech 1.0 döneminde, veri analizlerinin ve işlem izlemenin yaygınlaştığı RegTech 2.0 döneminde ve yapay zekâ, büyük veri, dağıtık defter teknolojisi, API vb. gibi günümüz teknolojilerinin kullanıldığı RegTech 3.0 döneminde teknolojik gelişmelere bağlı olarak sunulan çözümler değişmiş ve gelişmiştir.

Bu kapsamda çalışmada; krizler ve çeşitli nedenler ile artan düzenlemelere uyumda yaşanılan zorlukların aşılması için bankaların uyum riski yönetiminde kullandığı teknolojilerin incelenmesi, kullanılan çözümlerin bankalara, sektöre ve uyum riski denetimine etkisinin değerlendirilmesi ve vaka bazında örneklerin incelenmesi amaçlanmıştır.

Çalışmanın ilk bölümünde RegTech, uyum ve regülasyon kavramları, RegTech'in dönemlere göre gelişimi ve bu dönemlerdeki kullanılan teknolojiler anlatılmış, uyum riski ve RegTech konularında literatür taraması yapılmıştır.

Çalışmanın ikinci bölümünde bankacılıktaki uyum riskleri belirtilmiş, Türkiye bankacılık sektöründeki uyulması gereken düzenlemelere çeşitli örnekler verilmiş, uyum riski yönetiminin bileşenleri ve bu bileşenlerin denetimi değerlendirilmiş, denetim türleri, denetimin amacı ve kullanılan denetim modeli anlatılmıştır. Bankaların uyum programlarını belirleyerek uyum risklerini yönetmesi, organizasyonlarını IIA'in üçlü hat savunma modeline göre yapılandırması ve iç kontrol ortamını sağlaması uyum riski kaynaklı potansiyel zarar kayıplarını önleyecektir.

Çalışmanın üçüncü bölümünde, RegTech ekosistemi, sektörün geleceği, RegTech'in fayda ve zorlukları, kullanılan teknolojik altyapılar ve hangi alanlarda çözümler sunulduğu araştırılmış ve RegTech'in bankacılık ile ilişkisi değerlendirilmiştir. Yıllara sari bakıldığında 2017-2021 yılları arasında RegTech sektöründe yapılan anlaşmaların %181, yatırım tutarlarının ise %1160 arttığı ve RegTech pazarının da 2027 yılında 30,4 milyar $'a çıkmasının beklendiği görülmüştür. Finansal kurumların RegTech çözümlerini tasarruf etme, müşteri deneyimini iyileştirme, uyum riskini azaltma gibi tercih etme nedenlerinin yanı sıra düzenlemelerin standart olmaması, siber güvenlik alanındaki çekinceler, yeni teknolojilere yatırım yapmak için bütçe ayrılması gerektiği gibi nedenlerle de RegTech çözümlerine geçişte zorluklar yaşandığı belirtilmiştir.

Yapay zekâ, API, büyük veri, blok zinciri, bulut teknolojisi, otomasyon sistemleri gibi çeşitli teknolojilerden yararlanan RegTech firmaları geliştirdikleri ürünler ile AML/KYC süreçleri, risk yönetimi, yasal raporlamalar, işlem izleme süreçleri gibi birçok alanda uyum riskini azaltmak için çözümler getirdiği görülmüştür. Bu çözümlerin düzenlemelerin yoğun olduğu bankacılık sektöründe uygulanmasının bankaların uyum riski yönetimini daha etkin hale getireceği belirtilmiştir. Dijital bankacılığın gelişmeye başlaması ve açık bankacılık alanında düzenlemelerin yapılması RegTech çözümlerine olan ihtiyacı da ortaya koymuş ve açık bankacılığın gelişmesiyle birlikte RegTech sektörü de aynı yönlü gelişimini sürdürmüştür.

Çalışmanın son bölümünde uyum riskinin bankalara maliyeti ve uyumsuzluk sonucunda katlanılan maliyetler belirtilmiş, bu maliyetlerin azaltılması için

bankacılıkta kullanılabilecek uygulamalar vaka analizi ve örnekler ile anlatılmış ve Türkiye'de RegTech sektörünün gelişimi değerlendirilmiştir.

2008 krizi sonrasında bankacılık alanında düzenlemelerin arttığı ve buna bağlı olarak da maliyetlerin yükseldiği görülmektedir. The Trade'in yaptığı araştırmada bankalar sadece 2016 yılında yasal uyum için 100 milyar $'ın üstünde harcama yapmıştır. Mali suçlardaki uyum maliyetine bakıldığında ise Lexis Nexis'in 2021 yılı "True Cost Of Financial Crime Compliance Study" raporunda her bölgenin maliyetinin arttığı ve bu artışın %18,10 ila %61,30 arasında değiştiği tespit edilmiştir. Ukrayna-Rusya savaşı nedeniyle küresel olarak düzenlemelerin artması örneğinde olduğu gibi krizler, savaşlar, yeni teknoloji veya alanlar gibi çeşitli nedenlerle bankaların uyması gereken düzenlemelerin giderek artacağı, bunun da bankaların uyum maliyetini ve uyum riskini artıracağı için RegTech çözümlerine yöneleceği kanaatine varılmıştır.

Çalışmada uyumsuzluk durumlarında bankanın katlandığı maliyetler de belirtilmiş ve hem globalde hem de Türkiye'de çeşitli otoritelerin bankalara verdikleri cezalara örnekler verilmiştir. Financial Times'ın analizine göre 2008-2022 yılları arasında finansal kurumların toplamda 55 milyar $'a yakın kara para aklamayı önleme düzenlemeleri sebepli maliyete katlandıkları tespit edilmiştir. Bankalara AML süreçleri yanında kontrol eksikliği, yanlış raporlama, yaptırım ihlalleri gibi çeşitli konularda para cezalarının verildiği görülmüştür. Bu cezalar bankaları hem finansal hem de itibar açısından olumsuz etkilemekte ve Wegelin & Co örneğinde olduğu gibi bazı durumlarda bankanın kapatılmasına bile sebep olabilmektedir. Bu gibi durumlarla karşı karşıya kalmamaları için bankaların uyum riski yönetimini etkin bir şekilde yapmaları önemlidir.

Çalışmada ayrıca operasyonel riskler ile uyum riskleri birlikte değerlendirilerek uyum riskinin bankanın operasyonel süreçlerdeki yeri araştırılmıştır. Bankaların çeşitli durumlarda operasyonel süreçlerdeki eksiklik veya hatalar nedeniyle uyum riskine maruz kaldıkları tespit edilmiştir. AML/KYC gibi süreçlerin yanı sıra operasyonel riskin yönetilememesi Wells Fargo örneğinde olduğu gibi bankanın finansal ve itibar kaybıyla sonuçlanabilmektedir.

Wells Fargo vakasında bankanın daha fazla kar elde etme güdüsüyle uyguladığı satış politikası nedeniyle personellerine satış baskı kurarak operasyonel riske sebebiyet verdiği, iç kontrol ortamını sağlayamadığı, bunların neticesinde operasyonel risklerini yönetemediği ve uyum riskine maruz kalarak 8,5 milyar $ para cezası ödemek zorunda kaldığı tespit edilmiştir. Bu örnek, uyum riskinin sadece AML/KYC gibi süreçlerden oluşmadığı, bankaların operasyonel süreçlerinin yönetilememesi nedeniyle de büyük maliyetlere katlanmak zorunda kalabileceğini göstermektedir.

Bankalar operasyonel riskler nedeniyle uyum riskine maruz kalmamaları için banka içinde sağlam bir uyum kültürü oluşturmalı, düzenli olarak risklerini belirlemeli ve değerlendirmeli, güçlü politikalar oluşturmalı, uyum risklerini yönetmek için teknolojiden yardım almalı, personeli düzenli periyotlarda eğitmeli ve tüm süreçlerin etkinliğini izleyerek denetlemelidir.

Türkiye'de tüketici şikayetlerini belirli bir tutara kadar Tüketici Hakem Heyetleri kabul etmekte, finansal kuruluşlarca sağlanan bireysel ürün ve hizmetlerle ilgili şikayetleri ise BDDK Finansal Tüketici İlişkileri Daire Başkanlığı incelemektedir. Amerika'da bulunan Tüketici Finansal Koruma Bürosu kadar geniş yetkileri bulunan ve bankalara devasa para cezaları kesebilecek bir büro/kurum Türkiye'de bulunmamaktadır. Son yıllarda bankaların, finansal kurumların, FinTech'lerin, dijital bankacılığın, kripto para borsalarının…vb. hızlı artışı finans sektöründe şikayetleri de artırmıştır. Tüketici Finansal Koruma Bürosu örneğinde olduğu gibi sadece finans alanında uzmanlaşmış olan ve geniş yetkilere sahip bir kurumun Türkiye'de kurulması değerlendirilebilir.

Deloitte'un "RegTech Business Cases 2021" raporuna göre RegTech uygulamalarının %79'unun %30 üzeri zaman tasarrufu ve %75'inin ise %30 üzeri maliyet tasarrufu sağladığı, RegTech çözümlerindeki her alanda yüksek oranda API teknolojisinin kullanıldığı, uyum ve yasal raporlama alanlarında en fazla kullanılan ikinci teknolojinin bulut bilişim teknolojisi olduğu, kimlik yönetimi ve kontrolü ile risk yönetimi alanlarında en fazla kullanılan ikinci teknolojinin büyük veri teknolojisi olduğu, işlem izleme alanlarında ise bulut bilişim ve büyük veri teknolojilerinin eşit oranda kullanıldığı tespit edilmiştir.

Türkiye'de RegTech sektörüne bakıldığında sektörün oluşum aşamasında olduğu, Türkiye merkezli birkaç RegTech firmasının bulunduğu, uyum konusunda ise Türkiye'nin 2019 yılında FATF tarafından takip sürecine alındığı ve 2021 yılında ise FATF tavsiyelerine uyumu yeniden derecelendirilerek Gri Listeye alındığı görülmüştür. MASAK'ın 2021 yılı faaliyet raporuna bakıldığında, 2017-2021 yılları içerisinde 2019 yılında diğer yıllara göre daha az idari para cezası verildiği, 2021 yılında bir önceki yıla göre neredeyse 3 kat arttığı, bu dalgalanmanın yıllara göre yapılan denetimlerin sayısındaki değişiklikten kaynaklandığı tespit edilmiştir.

İç denetim ile RegTech arasındaki ilişkiye bakıldığında, günümüzde geleneksel denetimden risk bazlı uzaktan denetime ve çeşitli senaryolara dayalı merkezden denetim modellerine geçildiği, bu modellerde teknolojinin daha yoğun kullanıldığı, teknolojinin gelişmesiyle veri üretiminin gelecekte çok daha fazla olacağı, bu nedenle veri analizinde uzmanlaşmış kişilerin daha fazla istihdam edileceği, yapay zeka, büyük veri, robotik süreç otomasyonu gibi teknolojilerden yararlanan çeşitli RegTech çözümlerinin iç denetimde kullanılması ihtiyacının arttığı, böylelikle iç denetim birimlerinin çağa ayak uyduracağı ve etkin bir iç denetim yapılabileceği tespit edilmiştir.

Sonuç olarak; uyum riski yönetimi bankanın oluşturacağı uyum kültürüyle, her bir organının bu kültürü sahiplenmesiyle, üçlü hat savunma modelinin benimsenip iç kontrol ortamının sağlanarak riski en aza indirilmesiyle yapılacaktır. Uyum riskinin bankaya maliyeti ve uyumsuzluk sonucu oluşabilecek potansiyel finansal ve itibari kayıp azımsanmamalıdır. Bu maliyeti azaltmak ve riski önlemek RegTech çözümleri ile mümkün olacaktır.

KAYNAKÇA

Adl, M., Haworth W. C.: 2018 "How a Know-Your-Customer Utility Could Increase Access to Financial Services in Emerging Markets", **World Bank Group,** EMCompass, 59, 1-8, (Çevrimiçi) https://documents1.worldbank.org/curated/en/133091547846776274/pdf/133879-EMCompass-Note-59-KYC-Utility.pdf, 9 Mayıs 2023

Akın, E., Kalem, M.: 2009 "Müşterinin Tanınmasında Gerçek Faydalanıcının Tespiti", **Bankacılar Dergisi,** 68, 65-79, (Çevrimiçi) https://www.tbb.org.tr/Dosyalar/Arastirma_ve_Raporlar/musteritanimasi.pdf, 16 Nisan 2023

Aktan, E.: 2018 "Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu", **Ankara Üniversitesi Bilgi Yönetimi Dergisi**, Cilt 1, Sayı 1, 1-22

Aktas, E., Roland, K.: 2021 "Fintech Revolution, Regulatory And Supervisory Challenges, And Opportunities For Improvement By Utilizing Regtech And Suptech", **International Journal of Business Research and Information Technology**, 8/1, 87

Aljazeera: 2018 "Mehmet Hakan Atilla gets 32-month sentence in Iran sanctions case", **Aljazeera** (Çevrimiçi) https://www.aljazeera.com/news/2018/5/16/mehmet-hakan-atilla-gets-32-month-sentence-in-iran-sanctions-case, 29 Mayıs 2023

Alvantia: 2018 "Digital Banking – Neo Banks, ChallengerBanks & BaaS" (Çevrimiçi) https://www.alvantia.com/en/digital-banking-neo-banks-challengerbanks-baas/, 28 Mayıs 2023

Arasa, R., Ottichilo, L.: 2015 "Determinants of Know Your Customer (KYC) Compliance among Commercial Banks in Kenya", **Journal of Economics and Behavioral Studies,** 7/2, 162-175, (Çevrimiçi) https://doi.org/10.22610/jebs.v7i2(J).574, 10 Ekim 2022

Arner, D. W., Barberis J. N. ve Buckley R.P.: 2017 "FinTech and RegTech in a Nutshell, and the Future in a Sandbox.", **Research Foundation Briefs,** 3/4, 1-20, (Çevrimiçi) http://dx.doi.org/10.2139/ssrn.3088303, 20 Mayıs 2023

Arner, D. W., Barberis, J. N. ve Buckey, R. P.: 2015 "The evolution of Fintech: A new post-crisis paradigm.", **University of Hong Kong Faculty of Law Research Paper**, 2015/047, 1-44 (Çevrimiçi) https://ssrn.com/abstract=2676553, 20 Mayıs 2023

Arner, D. W., Barberis, J. N. ve Buckley, R. P.: 2016a "The Emergence of RegTech 2.0: From Know Your Customer to Know Your Data", **Journal of Financial Transformation**, 44, 79-86, (Çevrimiçi), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3044280#, 24 Şubat 2023

Ascent RegTech: 2023 "Open Banking: What It Is, Why It Matters, and How RegTech Can Help", **Ascent Regtech,** (Çevrimiçi) https://www.ascentRegTech.com/blog/open-banking-what-it-is-why-it-matters-and-how-RegTech-can-help/, 28 Mayıs 2023

Asenov, E.: 2015 "Characteristics of Compliance Risk in Banking", **Economic Alternatives,** 4, s.20-28. (Çevrimiçi) https://www.unwe.bg/uploads/Alternatives/2-Asenov.pdf, 10 Ekim 2022

Babuşcu, Ş.: 2005 "Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi", **Akademi Eğitim Yayıncılık**, İstanbul

BaFin: 2021 "Deutsche Bank AG: BaFin imposes administrative fine", **Federal Financial Supervisory Authority,** (Çevrimiçi) https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Massnahmen/40c_neu_124_WpHG/meldung_211229_deutsche_bank_ag_geldbusse_en.html#:~:text=On%2028%20December%202021%2C%20BaFin,EU%20)%202016%2F1011, 28 Mayıs 2023

Bankacılık Kanunu: 2005 "5411 sayılı Bankacılık Kanunu", (Çevrimiçi) https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5411&MevzuatTur=1&MevzuatTertip=5, 20 Mayıs 2023

Barrere, G.: 2020 "RegTech: Institutionalizing Compliance & A Better Customer Experience", **Performline,** (Çevrimiçi) https://performline.com/blog-post/RegTech-compliance-improved-customer-experience/, 27 Mayıs 2023

BCBS, t.y. (a) "History of the Basel Committee", **Basel Committee on Banking Supervision,** (Çevrimiçi) https://www.bis.org/bcbs/history.htm, 10 Mayıs 2023

BCBS, t.y. (b) "The Basel Committee - overview", **Basel Committee on Banking Supervision,** (Çevrimiçi) http://www.bis.org/bcbs/, 10 Mayıs 2023

BCBS: 2005 "Compliance and the compliance function in banks", **Basel Committee on Banking Supervision,** 1-16 (Çevrimiçi) https://www.bis.org/publ/bcbs113.htm, 16 Şubat 2023

BCBS: 2018 "Sound Practices: implications of fintech developments for banks and bank supervisors", **Basel Committee on Banking Supervision,** 1-49 (Çevrimiçi) https://www.bis.org/bcbs/publ/d431.htm, 27 Mayıs 2023

BCBS: 2022 "Calculation of RWA for operational risk" **Basel Committee on Banking Supervision,** 1-9 (Çevrimiçi) https://www.bis.org/basel_framework/chapter/OPE/10.htm?tldate=20221231&inforce=20220101&published=20191215, 28 Mayıs 2023

BDDK, t.y. "Mevzuat", **BDDK,** (Çevrimiçi) https://www.bddk.org.tr/Mevzuat/Index/4, 29 Mayıs 2023

BDDK: 2016 "Operasyonel Riskin Yönetimine İlişkin Rehber", **BDDK**, 1-24 (Çevrimiçi) https://www.bddk.org.tr/Mevzuat/DokumanGetir/948, 18 Nisan 2023

BDDK: 2021 "2021 Faaliyet Raporu" **BDDK**, 1-94 (Çevrimiçi) https://www.bddk.org.tr/KurumHakkinda/EkGetir/5?ekId=133, 28 Mayıs 2023

Bignell, F.: 2023 "Global Fintech Investment in 2023 – Why the Industry Remains Optimistic Following a Tough 2022", **The Fintech Times,** (Çevrimiçi) https://thefintechtimes.com/global-fintech-investment-in-2023-why-the-industry-remains-optimistic-following-a-tough-2022/, 28 Mayıs 2023

Bilham, J.: 2022 "Neobank Design: 3 Great Examples in a New Era of Banking" **Raw.Studio,** (Çevrimiçi) https://raw.studio/blog/3-great-examples-of-neobank-design/, 28 Mayıs 2023

Birindelli, G., Feretti, P.: 2008 "Compliance risk in Italian banks: the results of a survey", **Journal of Financial Regulation and Compliance**, 16/4, 335-351 (Çevrimiçi) https://doi.org/10.1108/13581980810918404, 10 Ekim 2022

Bloomberght: 2022 "TCMB'den bankalara yurt dışına transferlerde şeffaflık uyarısı", **Bloomberght,** (Çevrimiçi) https://www.bloomberght.com/tcmb-den-bankalara-yurt-disina-transferlerde-seffaflik-uyarisi-2321685, 29 Mayıs 2023

Bloomberght: 2023a "TCMB'den bankalara 700 milyon liralık döviz cezası" **Bloomberght,** (Çevrimiçi) https://www.bloomberght.com/tcmbden-bankalara-700-milyon-liralik-doviz-cezasi-2325830, 29 Mayıs 2023

Bloomberght: 2023b "Halkbank'tan tazminat davası açıklaması" **Bloomberght,** (Çevrimiçi) https://www.bloomberght.com/halkbank-tan-abd-deki-tazminat-talepli-hukuk-davasina-iliskin-2330680, 29 Mayıs 2023

Bodoni, S., Browning, J.: 2022 "Santander Hit by UK Fine for Lax Money-Laundering Controls", **Bloomberg,** (Çevrimiçi)

https://www.bloomberg.com/news/articles/2022-12-09/santander-fined-107-million-in-uk-anti-money-laundering-probe, 26 Mayıs 2023

Bodoni, S., Browning, J.: 2022 "Santander Hit by UK Fine for Lax Money-Laundering Controls", **Bloomberg**, (Çevrimiçi) https://www.bloomberg.com/news/articles/2022-12-09/santander-fined-107-million-in-uk-anti-money-laundering-probe, 28 Mayıs 2023

BoE: 2021 "Final Notice", **Bank of England Prudential Regulation Authority**, 1-40 (Çevrimiçi) https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/regulatory-action/final-notice-from-pra-to-standard-chartered-bank.pdf, 28 Mayıs 2023

Bozan, E.: 2022 "Masrafsız ve Şubesiz Bankacılık için 7 Alternatif", **Konu Para**, (Çevrimiçi) https://konupara.com/kisisel-finans/subesiz-bankacilik-icin-7-alternatif-4485/, 20 Mayıs 2023

Buckley, R. P., Arner, D. W., Zetzsche, D. A., Weber, R. H.: 2020 "The road to RegTech: The (astonishing) example of the European Union", **Journal of Banking Regulation**, 21/1, 26–36, (Çevrimiçi) https://doi.org/10.1057/s41261-019-00104-1, 20 Mayıs 2023

Butler, T., O'Brien, L.: 2019 "Understanding RegTech for digital regulatory compliance. Disrupting finance: FinTech and strategy in the 21st century", **Palgrave Studies in Digital Business & Enabling Technologies**, 85-100 (Çevrimiçi) http://dx.doi.org/10.1007/978-3-030-02330-0_6, 28 Mayıs 2023

Büchner, A. G., Mulvenna, M. D.: 1998 "Discovering Internet marketing intelligence through online analytical web usage mining", **ACM Sigmod Record**, 27/4, 59-61, (Çevrimiçi) https://doi.org/10.1145/306101.306124, 28 Mayıs 2023

Can, E.: 2003 "Operasyonel Risk ve Yönetimi", **Sermaye Piyasası Kurulu Yayınları**, Ankara, 1-50 (Çevrimiçi)

https://spk.gov.tr/data/61e48fc71b41c60d1404d68a/89a6be777006864194aabe08adbec31c.pdf, 20 Mayıs 2023

CBinsight: 2022 "The challenger bank playbook: How 6 digital banking upstarts are taking on retail banking", **CBinsight**, (Çevrimiçi) https://www.cbinsights.com/research/report/challenger-bank-playbook/, 28 Mayıs 2023

CBinsights, t.y. "Mindbridge", **CBinsight,** (Çevrimiçi) https://www.cbinsights.com/company/mindbridge-ai, 29 Mayıs 2023

CBinsights: 2017 "Regtech Market Map: The Startups Helping Businesses Mitigate Risk And Monitor Compliance Across Industries", **CBinsight,** (Çevrimiçi) https://www.cbinsights.com/research/RegTech-regulation-compliance-market-map/, 27 Mayıs 2023

CFTC, 2021 "CFTC Orders JPMorgan to Pay $75 Million for Widespread Use by Employees of Unapproved Communication Methods and Related Recordkeeping and Supervision Failures", **Commodity Futures Trading Commission,** (Çevrimiçi) https://www.cftc.gov/PressRoom/PressReleases/8470-21, 28 Mayıs 2023

Chang, E.: 2023 "What Is a Neobank?", **USNews,** (Çevrimiçi) https://money.usnews.com/banking/articles/what-is-a-neobank, 20 Mayıs 2023

Christidis, K., Devetsikiotis, M.: 2016. "Blockchains and smart contracts for the internet of things**" IEEE Access**, 4, 2292-2303 (Çevrimiçi) https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408, 28 Mayıs 2023

Clark, G., Ziemba, R., Dubowitz, M.: 2013 "Iran's Golden Loophole", **Roubini Global Economics**, 1-11 (Çevrimiçi), https://s3.us-east-

2.amazonaws.com/defenddemocracy/uploads/documents/FDD_RGE_Iran_GoI_Report__May_2013_FINAL_2.pdf, 29 Mayıs 2023

Comfort, N., Arons, S.: 2021 "Deutsche Bank Fined $9.8 Million by BaFin for Control Lapses", **Bloomberg,** (Çevrimiçi) https://www.bloomberg.com/news/articles/2021-12-29/deutsche-bank-faces-9-8-million-fine-by-german-finance-watchdog#:~:text=Germany's%20finance%20watchdog%20fined%20Deutsche,scandal%20that%20rocked%20the%20industry, 26 Mayıs 2023

Comfort, N., Arons, S.: 2021 "Deutsche Bank Fined $9.8 Million by BaFin for Control Lapses", **Bloomberg,** (Çevrimiçi) https://www.bloomberg.com/news/articles/2021-12-29/deutsche-bank-faces-9-8-million-fine-by-german-finance-watchdog, 28 Mayıs 2023

Comply Advantage: 2022 "Why is RegTech Important to Adopt?", **Comply Advantage,** (Çevrimiçi), https://complyadvantage.com/insights/why-is-regtech-adoption-important/, 27 Mayıs 2023

Cowburn, N., Barnet, P.: 2019 "RegTech Opportunities in a Post-4MLD/5MLD World", **The RegTech Book**, John Wiley & Sons, 172-177

Dahl, D., Meyer, A., Neely, M.: 2016 "Scale Matters: Community Banks and Compliance Costs", **The Regional Economist**, 1-3. (Çevrimiçi) https://www.stlouisfed.org/~/media/Publications/Regional-Economist/2016/July/scale_matters.pdf, 10 Ekim 2022

Deloitte, t.y.(a) "Modernizing the three lines of defense model", **Deloitte** (Çevrimiçi) https://www2.deloitte.com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model.html, 15.03.2023

Deloitte, t.y.(b) "RegTech Universe 2023", **Deloitte** (Çevrimiçi) https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html, 27 Mayıs 2023

Deloitte: 2017a "The Future of Regulatory Productivity, powered by RegTech. RegTech position paper, Financial Service", **Deloitte**, (Çevrimiçi) https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-regulatory-future-of-regulatory-productivity-powered-by-regtech.pdf, 24 Şubat 2023

Deloitte: 2017b "The RegTech universe on the rise", **Inside Magazine- Edition,** 68-79, (Çevrimiçi) https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/about-deloitte/Inside/lu_inside-global-edition-2017-full.pdf, 24 Şubat 2023

Deloitte: 2018a "The case for artificial intelligence in combating money laundering and terrorist financing", **Deloitte,** 1-38, (Çevrimiçi), https://www2.deloitte.com/tr/en/pages/financial-advisory/articles/the-case-for-artificial-intelligence-in-combating-money-laundering-and-terrorist-financing.html, 20 Mayıs 2023

Deloitte: 2018b "Using RegTech to transform compliance and risk from support functions into business differentiators", **Inside Magazine- Edition**, 1-8, (Çevrimiçi), https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-using-RegTech-to-transform-compliance-and-risk-from-support-functions-into-business-differentiators.pdf, 24 Şubat 2023

Deloitte: 2021 "Regtech Business Cases 2021: Explore the tangible value of Regtech solutions", **Deloitte,** (Çevrimiçi) https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html, 28 Mayıs 2023

EBA: 2021a "Analysis of RegTech in the EU Financial Sector", **European Banking Authority**, EBA/Rep/2021/17, (Çevrimiçi) https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1015484/EBA%20analysis%20of%20RegTech%20in%20the%20EU%20financial%20sector.pdf, 11 Mayıs 2023

EBA: 2021b "Discussion paper on machine learning for IRB models", **European Banking Authority,** EBA/DP/2021/04, (Çevrimiçi) https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Discussions/2022/Discussion%20on%20machine%20learning%20for%20IRB%20models/1023883/Discussion%20paper%20on%20machine%20learning%20for%20IRB%20models.pdf, 11 Mayıs 2023

EBA: 2021c "Study of the Cost of Compliance with Supervisory Reporting Requirements", **European Banking Authority,** EBA/Rep/ 2021/15, (Çevrimiçi) https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1013948/Study%20of%20the%20cost%20of%20compliance%20with%20supervisory%20reporting%20requirement.pdf, 11 Mayıs 2023

Egan, M.: 2017 "Wells Fargo Dumps Toxic 'Cross-Selling' Metric", **CNN Money**, (Çevrimiçi), http://money.cnn.com/2017/01/13/investing/wells-fargocross-selling-fake-accounts/index.html., 28 Mayıs 2023

Elliehausen, G.: 1998 "The cost of Bank regulation: A Review of the Evidence", **Board of Governors of the Federal Reserve System**, Washington, DC 20551, 1-33, (Çevrimiçi) https://www.researchgate.net/publication/5039973_The_cost_of_banking_regulation_a_review_of_the_evidence, 28 Mayıs 2023

Elson, R. J., Ingram, P.: 2018 "Wells Fargo and the unauthorized customer accounts: A case study", **Global Journal of Business Pedagogy**, 2/1, 124-133, (Çevrimiçi) https://www.igbr.org/wp-content/uploads/articles/GJBP_Vol_2_No_1_2018-pgs-124-133.pdf, 28 Mayıs 2023

Er, S.: 2010 "5018 Sayılı Kanun Karşısında Düzenleyici ve Denetleyici Kurumların Konumu"**, Dış Denetim,** 183-191

Ergül, E.: 2001 "Karapara Ensdüstrisi ve Aklama Suçu", **Yargı Yayınevi**, İstanbul, 58,

Everson, M., Ilako, C., Florio, C.D.: 2003 "Corporate Governance, Corporate Governance, Business Ethics, and Business Ethics, and Global Compliance Management**", ABA Bank Compliance**, 22-32 (Çevrimiçi) https://silo.tips/download/corporate-governance-business-ethics-and-global-compliance-management, 25 Mayıs 2023

EY: 2019 "Regulatory technology (RegTech)", **Ernst & Young,** (Çevrimiçi) https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/financial-services/ey-regulatory-technology-regtech.pdf, 27 Mayıs 2023

EY: 2021 "Compliance transformation: how banks can leverage opportunities now", **Ernst & Young,** (Çevrimiçi) https://www.ey.com/en_tr/banking-capital-markets-risk-regulatory-transformation/compliance-transformation-how-banks-can-leverage-opportunities-now, 10 Ekim 2022

FATF, t.y. "FATF 40 Recommendations", **Financial Action Task Force**, (Çevrimiçi) https://www.cfatf-gafic.org/documents/fatf-40r, 14 Mart 2023

FATF: 2023 "Jurisdictions under Increased Monitoring- 24 February 2023", **Financial Action Task Force,** (Çevrimiçi) https://www.fatf-

gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2023.html, 28 Mayıs 2023

FCA: 2016 "Call for input on supporting the development and adopters of RegTech", **Financial Conduct Authority** (Çevrimiçi) https://www.fca.org.uk/publication/feedback/fs-16-04.pdf, 28 Mayıs 2023

FCA: 2022 "FCA fines Santander UK £107.7 million for repeated anti-money laundering failures", **Financial Conduct Authority** (Çevrimiçi) https://www.fca.org.uk/news/press-releases/fca-fines-santander-uk-repeated-anti-money-laundering-failures, 28 Mayıs 2023

FED: 2023 "Order of Assessment of Civil Money Penalty Issued Upon Consent Pursuant to the Federal Deposit Insurance Act, as Amended", **Federal Reserve System,** (Çevrimiçi) https://www.federalreserve.gov/newsevents/pressreleases/files/enf20230330a1.pdf, 28 Mayıs 2023

Figliola P. M.: 2020 "The Internet of Things (IoT): An Overview", **Congressional Research Service (CRS)**, (Çevrimiçi) https://crsreports.congress.gov/product/pdf/IF/IF11239, 28 Mayıs 2023

Financial Stability Board: 2017 "Artificial intelligence and machine learning in financia lservices", **Financial Stability Board** (Çevrimiçi) https://www.fsb.org/wp-content/uploads/P011117.pdf, 28 Mayıs 2023

Fineksus, t.y.(a) "Difference between Fintech and Regtech", **Fineksus,** (Çevrimiçi) https://fineksus.com/difference-between-fintech-and-RegTech/, 27 Mayıs 2023

Fineksus, t.y.(b) "The 2022 Surge in Anti-Money Laundering Fines: A Closer Look at the Top 5 Penalties", **Fineksus,** (Çevrimiçi) https://fineksus.com/the-

2022-surge-in-anti-money-laundering-fines-a-closer-look-at-the-top-5-penalties/, 28 Mayıs 2023

Fineksus/Fintech İstanbul: 2020 "AML Strateji Rehberi", **Fineksus / Fintech İstanbul,** (Çevrimiçi) https://fineksus.com/landing_page/aml/tr/, 24 Şubat 2023

Fintech Global, t.y. "About FinTech Global", **Fintech Global** (Çevrimiçi) https://fintech.global/about/, 28 Mayıs 2023

Fintech Global: 2022 "RegTech funding more than doubled in 2021, led by large cybersecurity deals", **Fintech Global** (Çevrimiçi) https://fintech.global/2022/01/12/RegTech-funding-more-than-doubled-in-2021-led-by-large-cybersecurity-deals/, 27 Mayıs 2023

Fintech İstanbul: 2019 "Dünyada ve Türkiyede Açık Bankacılık: Bankacılığın Geleceği" **Rumi Matbaacılık,** İstanbul, Edt. Özlem Özkan, (Çevrimiçi) https://bkm.com.tr/wp-content/uploads/2015/06/Dunyadaveturkiyedeacikbankacilik.pdf, 28 Mayıs 2023

Fintech İstanbul: 2021 "Bankaların dijital müşteri edinimine ilişkin düzenleme 1 Mayıs'ta yürürlüğe giriyor" **Fintech İstanbul,** (Çevrimiçi) https://fintechistanbul.org/2021/04/02/bankalarin-dijital-musteri-edinimine-iliskin-duzenleme-1-mayista-yururluge-giriyor/, 16 Mayıs 2023

Fintech İstanbul: 2022a "BirAPI, Open Banking Turkiye Monitor Public API's verilerini yayınladı", **Fintech İstanbul,** (Çevrimiçi) https://fintechistanbul.org/2022/08/08/birapi-open-banking-turkiye-public-apis/, 28 Mayıs 2023

Fintech İstanbul: 2022b "Ödeme sistemlerinde 2023'e yön verecek 7 trend", **Fintech İstanbul**, (Çevrimiçi) https://fintechistanbul.org/2022/12/26/odeme-sistemlerinde-2023e-yon-verecek-7-trend/, 28 Mayıs 2023

Fintech İstanbul: 2022c "Türkiye'nin ilk şubesiz dijital bankası Hayat Katılım, kuruluş iznini aldı", **Fintech İstanbul,** (Çevrimiçi) https://fintechistanbul.org/2022/04/22/turkiyenin-ilk-subesiz-dijital-bankasi-hayat-katilim-kurulus-iznini-aldi/, 20 Mayıs 2023

Fintech İstanbul: 2023 "Türkiye'de bankacılıkta 14 milyon KYC başvurusu", **Fintech İstanbul,** (Çevrimiçi) https://fintechistanbul.org/2023/01/18/turkiyede-bankacilikta-14-milyon-kyc-basvurusu/, 28 Mayıs 2023

Gabbi, G., Tanzi, P. M., ve Nadotti, L.: 2011 "Firm size and compliance costs asymmetries in the investment services", **Journal of Financial Regulation and Compliance**, 19/1, 58-74. (Çevrimiçi) https://doi.org/10.1108/13581981111106176, 10 Ekim 2022

Gillis, A. S.: 2022 "What is the internet of things (IoT)?", **TechTarget,** (Çevrimiçi) https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT, 28 Mayıs 2023

Güredin, E.: 2008 "Denetim ve Güvence Hizmetleri", **Türkmen Kitabevi,** İstanbul, 13. Baskı

Gürkan, M. A.: 2021 "Siber Güvenlik ve Covid 19 Salgının Uzaktan Denetim Üzerinde Etkileri", **Denetişim,** 22, 27-39, (Çevrimiçi) https://search.trdizin.gov.tr/yayin/detay/438352, 16 Mart 2023

Hayes, A.: 2022 "What Is Cross-Selling?", **Investopedia,** (Çevrimiçi) https://www.investopedia.com/terms/c/cross-sell.asp, 28 Mayıs 2023

Haynes, A.: 2005 "The effective articulation of risk-based compliance in banks", **Journal of Banking Regulation**, 6, 146-162 (Çevrimiçi) https://doi.org/10.1057/palgrave.jbr.2340188, 10 Ekim 2022

Hill, J.: 2018 "Fintech and the remaking of financial institutions.", **Elsevier Science,** (Çevrimiçi)

https://discovery.ebsco.com/linkprocessor/plink?id=95230e16-08a2-3bf2-adab-ed2621bdf7f5, 24 Şubat 2023

Hugé F.K., Duprel C., Pescatore G.: 2017 "The Promise of RegTech: Elevating regulatory risk management in the financial industry to an effective business management practice", **Inside Magazine – European Union Edition,** 1-6, (Çevrimiçi) http://www.gaco.gi/images/pdf/2017-june/lu-the-promise-regtech-27032017.pdf, 28 Mayıs 2023firma

IIA: 2020 "IIA'nın Üçlü Hat Modeli" **The Institute of Internal Auditors**, 1-11, (Çevrimiçi) https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-turkish.pdf, 10 Nisan 2023

Initium, t.y. "Regtech — Why Financial Compliance is Moving to the Cloud", **Initium,** (Çevrimiçi) https://stories.initium.group/RegTech-why-financial-compliance-is-moving-to-the-cloud/, 28 Mayıs 2023

Institute of International Finance: 2015 "RegTech: Exploring Solutions for Regulatory Challenges", **Institute of International Finance,** (Çevrimiçi), https://www.iif.com/Publications/ID/4229/Regtech-Exploring-Solutions-for-Regulatory-Challenges, 24 Şubat 2023

Institute of International Finance: 2016 "RegTech in Financial Services: Technology Solutions for Compliance and Reporting", **Institute of International Finance,** (Çevrimiçi) https://www.iif.com/portals/0/Files/content/RegTech%20in%20Financial%20Servies.pdf, 28 Mayıs 2023

Institute of International Finance: 2017 "Deploying RegTech against Financial Crime", **Institute of International Finance,** (Çevrimiçi) https://www.iif.com/portals/0/Files/private/32370132_aml_final_id.pdf, 28 Mayıs 2023

İç Denetim: 2017 "Türk Bankacılığında Uyum Faaliyetleri", **İç Denetim** (Çevrimiçi) https://www.icdenetim.net/turk-bankaciliginda-uyum-faaliyetleri/, 29 Mayıs 2023

Johl, J.: 2022 "What are APIs and how do APIs work?", **MuleSoft,** (Çevrimiçi) https://blogs.mulesoft.com/learn-apis/api-led-connectivity/what-are-apis-how-do-apis-work/, 27 Mayıs 2023

Johnson, K., Freifeld, K. Landauro, I.: 2018 "Societe Generale to pay $1.4 billion to settle cases in the U.S.", **Reuters,** (Çevrimiçi) https://www.reuters.com/article/us-usa-fed-socgen-idUSKCN1NO26B, 28 Mayıs 2023

Johnson, K., Freifeld, K. ve Landauro, I.: 2018 "Societe Generale to pay $1.4 billion to settle cases in the U.S." **Reuters,** (Çevrimiçi) https://www.reuters.com/article/us-usa-fed-socgen-idUSKCN1NO26B, 26 Mayıs 2023

Kagermann, H., Kinney, W., Küting, K., Weber, C. P.: 2008 "Internal Audit Handbook: Management with the SAP®-audit roadmap**", Springer Berlin Heidelberg**, Berlin, Heidelberg.

Kara, D., Yaşar, O. Sundu, M.: 2019 "Örgütlerde Büyük Veri Analizi: Bankacılık Sektöründe Bir Araştırma", **6. International Management Information Systems Conference "Connectedness and Cybersecurity"**, Kadir Has Üniversitesi, İstanbul, (Çevrimiçi) https://www.academia.edu/40712127/%C3%96rg%C3%BCtlerde_B%C3%BCy%C3%BCk_Veri_Analizi_Bankac%C4%B1l%C4%B1k_Sekt%C3%B6r%C3%BCnde_Bir_Ara%C5%9Ft%C4%B1rma, 29 Mayıs 2023

Karaduman, D.: 2013 "Türkiye'de Karapara Aklama ile Mücadele Yöntemleri", **Yayınlanmış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı**, İstanbul,

Katara A.: 2018 "RPA as a Compliance Enabler – Exciting Times Ahead", **Tata Consultancy Services,** (Çevrimiçi)

https://www.tcs.com/content/dam/global-tcs/en/pdfs/insights/whitepapers/RPA-Compliance-Enabler.pdf, 28 Mayıs 2023

KPMG: 2018 "There's a revolution coming- Embracing the challenge of RegTech 3.0.", **KPMG,** (Çevrimiçi) https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2018/09/RegTech-revolution-coming.pdf, 24 Şubat 2023

Kurnia, S., Peng, F. Liu, Y. R.: 2010 "Understanding the adoption of electronic banking in China", **In 2010 43rd Hawaii International Conference on System Sciences,** 1-10 (Çevrimiçi) https://ieeexplore.ieee.org/document/5428460, 20 Mayıs 2023

Kurum, E.: 2020 "RegTech solutions and AML compliance: what future for financial crime?", **Journal of Financial Crime,** (Çevrimiçi) https://doi.org/10.1108/JFC-04-2020-0051, 26.03.2023

KVKK: 2016 "Kişisel Verilerin Korunması Kanunu", (Çevrimiçi) https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf, 19.04.2023

Lagzdins, A., Sloka, B.: 2012 "Compliance program in Latvias' banking sector: the results of a survey", **European Integration Studies**, 6, 225-232 (Çevrimiçi) https://pdfs.semanticscholar.org/e555/caa0702cb9375b35939cfc5a05995b3f3e95.pdf, 10 Şubat 2023

Lang, H.: 2023 "Wells Fargo to pay $97 mln for sanctions compliance failures", **Reuters** (Çevrimiçi) https://www.reuters.com/business/finance/wells-fargo-pay-97-mln-sanctions-compliance-failures-2023-03-30/, 26 Mayıs 2023

Leblebici Teker, D.: 2006 "Bankalarda Operasyonel Risk Yönetimi, Örnek Banka Uygulamalı", **Literatür Yayıncılık**, İstanbul

Levitt, H., Bain, B.: 2021 "JPMorgan Bosses Hooked on WhatsApp Fuel $200 Million Penalty", **Bloomberg,** (Çevrimiçi) https://www.bloomberg.com/news/articles/2021-12-17/jpmorgan-bosses-addicted-to-whatsapp-fuel-200-million-in-fines, 26 Mayıs 2023

LexisNexis: 2021 "True Cost Of Financial Crime Compliance Study", **LexisNexis Risk Solutions,** (Çevrimiçi) https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report, 28 Mayıs 2023

LexisNexis: 2022 "FCA approach to regtech", **LexisNexis Risk Solutions,** (Çevrimiçi) https://www.lexisnexis.co.uk/legal/guidance/regtech, 27 Mayıs 2023

Linda, J., Bailey, E.: 2022 "How RegTech can transform your business?", **KPMG**, (Çevrimiçi) https://kpmg.com/dp/en/home/media/press-releases/2022/02/how-regtech-can-transform-your-business.html, 27 Mayıs 2023

Losiewicz-Dniestrzanska, E.: 2015 "Monitoring of Compliance Risk in the Bank", **Procedia Economics and Finance,** 26, 800-805, (Çevrimiçi) https://doi.org/10.1016/S2212-5671(15)00846-1, 10 Ekim 2022

Ludwick, K.: 2006 "Tackling risk-based compliance", **Journal of Investment Compliance,** 7/4, 61-64, (Çevrimiçi) https://doi.org/10.1108/15285810610719961, 10 Ekim 2022

Marr, B.: 2018 "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read", **Forbes,** (Çevrimiçi) https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=4d70403060ba, 29 Mayıs 2023

MASAK: 2021 "T. C. Hazine ve Maliye Bakanlığı Mali Suçları Araştırma Kurulu Başkanlığı Faaliyet Raporu", **MASAK,** (Çevrimiçi)

https://ms.hmb.gov.tr/uploads/sites/12/2022/03/Faaliyet-Raporu-2021.pdf, 04 Şubat 2023

Mavral, Ü.: 2001 "Kara Para Kayıt Dışı Ekonomi İlişkisi ve Türkiye'ye Yansımaları", **Vergi Denetmenleri Derneği**, 57

McDowell, H.: 2017 "Banks spent close to $100 billion on compliance last year", **The Trade News,** (Çevrimiçi) https://www.thetradenews.com/banks-spent-close-to-100-billion-on-compliance-last-year/, 21 Mayıs 2023

Mell P. ve Grance T.: 2011 "The NIST Definition of Cloud Computing", **National Institute of Standards and Technology (NIST)**, (Çevrimiçi) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, 28 Mayıs 2023

Memminger, M., Baxter, M., Lin, E.: 2016 "Banking Regtechs to the Rescue?", **BAIN&COMPANY,** (Çevrimiçi) https://www.bain.com/insights/banking-RegTechs-to-the-rescue, 28 Mayıs 2023

Michaels, L., Homer, M.: 2018 "Regulation and supervision in a digital and inclusive world", **Handbook of Blockchain, Digital Finance, and Inclusion,** 1, 329–346

Micheler, E., Whaley, A.: 2020 "Regulatory technology: Replacing law with computer code", **European Business Organization Law Review**, 21/2, 349–377

Microsoft Azure, t.y. "What Is Cloud Computing? A Beginner's Guide", **Microsoft,** (Çevrimiçi) https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing, 28 Mayıs 2023

Mindbridge, t.y. "Mindbridge", (Çevrimiçi) https://www.mindbridge.ai/platform/technology/, 29 Mayıs 2023

Mulder, B. J. M.: 2019 "RegTech: Tackling Regulation with Innovation", **The RegTech Book, John Wiley & Sons,** 26-30

Myfico, t.y. "Relationship between Credit Cards and Credit Scores", **Myfico** (Çevrimiçi) https://www.myfico.com/credit-education/faq/cards/credit-cards-credit-score, 28 Mayıs 2023

Nakamoto, S.: 2008 "Bitcoin: A Peer-to-Peer Electronic Cash System", **Decentralized Business Review**, 21260 (Çevrimiçi) https://bitcoin.org/bitcoin.pdf, 28 Mayıs 2023

Natarajan, H., Krause S. K., Gradstein H. L.: 2017 "Distributed Ledger Technology (DLT) and blockchain", **World Bank Group,** Washington, (Çevrimiçi) https://openknowledge.worldbank.org/server/api/core/bitstreams/5166f335-35db-57d7-9c7e-110f7d018f79/content, 28 Mayıs 2023

Nguyen, G.: 2017 "RegTech: A few things in-house lawyers should know." **The Australian Corporate Lawyer Magazine**, 28/4, 32-33 (Çevrimiçi) https://www.acc.com/sites/default/files/resources/upload/RegTech.pdf, 27 Mayıs 2023

Nicolas, S., May, P. V.: 2017 "Building an effective compliance risk assessment programme for a financial institution", **Journal of Securities Operations & Custody**, 9/3, 215-224, (Çevrimiçi) https://www.henrystewartpublications.com/sites/default/files/Nicolas%2C%20Stephanie%20%26%20May%2C%20Paul%20JSOC%209-3.pdf, 10 Ekim 2022

Noonan, L., Smith, A.: 2023 "Global anti-money laundering fines surge 50%", **Financial Times**, (Çevrimiçi) https://www.ft.com/content/7a4821e6-96f1-475c-ae55-6401e402061f, 28 Mayıs 2023

Nsundano P. M.: 2007 "Comparatıve Legal Analysıs Of The Contemporary Treatment Of Money Launderıng Under The Jurısdıctıon Of Namıbıa and South Afrıca", **Yayımlanmamış Yüksek Lisans Tezi**, Faculty of Law University of Namibia, Namibia,

Nzuva S.: 2019 "Smart Contracts Implementation, Applications, Benefits, and Limitations", **Journal of Information Engineering and Applications**, 9/5, 63-75, (Çevrimiçi) https://www.researchgate.net/publication/336369143_Smart_Contracts_Implementation_Applications_Benefits_and_Limitations, 28 Mayıs 2023

OFAC: 2023 "OFAC Settles with Wells Fargo Bank, N.A. for $30,000,000 Related to Apparent Violations of Three Sanctions Programs" **OFAC**, (Çevrimiçi) https://ofac.treasury.gov/media/931541/download?inline, 28 Mayıs 2023

Oğuz, F.: 2011 "Devlet ve piyasa: Regülasyon ekonomisine giriş", **Seçkin Yayıncılık**, İstanbul, 16-19

Payne, P.: 2017 "Lawsuit: Petaluma Wells Fargo Employees 'Corralled' Day Laborers", **The Press Democrat,** (Çevrimiçi) https://www.pressdemocrat.com/article/news/lawsuit-petaluma-wells-fargo-employees-corralled-day-laborers/, 28 Mayıs 2023

Planet Compliance, t.y. "The Application of Blockchain Technology in the RegTech Sector", **Planet Compliance,** (Çevrimiçi) https://www.planetcompliance.com/the-application-of-blockchain-technology-in-the-RegTech-sector/#RegTech_and_Blockchain, 28 Mayıs 2023

Prove: 2021 "Growing Regulatory Complexities – RegTech to the Rescue", **Prove** (Çevrimiçi) https://www.prove.com/blog/growing-regulatory-complexities-RegTech-to-rescue, 28 Mayıs 2023

Prove: 2022 "How European Banks Are Using RegTech Solutions", **Prove,** (Çevrimiçi) https://www.prove.com/blog/how-european-banks-are-using-regtech-solutions, 15 Şubat 2023

Rajbhandari, A.: 2021 "SocGen CEO Takes Over Compliance After $2.6 Billion Fines", **Bloomberg,** (Çevrimiçi) https://www.bloomberg.com/news/articles/2021-12-10/socgen-ceo-oudea-takes-on-compliance-after-settlement-expires, 28 Mayıs 2023

Ramnarayan, A.: 2021 "StanChart fined $61.5 mln for misreporting liquidity position", **Reuters,** (Çevrimiçi) https://www.reuters.com/business/finance/bank-england-fines-standard-chartered-615-mln-regulatory-lapses-2021-12-20/, 28 Mayıs 2023

Rampton J.: 2023 "Everything You Need to Know about RegTech – The New Fintech", **Due,** (Çevrimiçi) https://due.com/everything-need-RegTech-new-fintech/#The_RegTech_ecosystem, 27 Mayıs 2023

Ranger, S.: 2022 "What is cloud computing? Everything you need to know about the cloud explained", **Zdnet** (Çevrimiçi) https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/, 28 Mayıs 2023

Raymond, N., Browning, L.: 2013 "Swiss bank Wegelin to close after guilty plea", **Reuters** (Çevrimiçi) https://www.reuters.com/article/us-swissbank-wegelin-idUSBRE9020O020130104, 28 Mayıs 2023

Regnology: 2022 "Blockchain in RegTech,", **Regnology** whitepaper, 3-4 (Çevrimiçi) https://www.regnology.net/ecomaXL/files/Regnology_Whitepaper_Blockchain-in-RegTech.pdf?download=1&item=26029, 28 Mayıs 2023

RegTech Analyst, Fintech Global: 2022 "Regtech100", **RegTech Analyst ve Fintech Global,** 11-84 (Çevrimiçi) https://fintech.global/regtech100/, 28 Mayıs 2023

Researchandmarkets: 2023 "RegTech Global Global Market Report 2023", **Researchandmarkets**, (Çevrimiçi) https://www.researchandmarkets.com/reports/5766986/RegTech-global-global-market-report, 27 Mayıs 2023

Resmi Gazete: 2012 "Bankaların İç Sistemleri Hakkında Yönetmelik", **Resmi Gazete,** (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2012/06/20120628-17.htm, 15 Mayıs 2023

Resmi Gazete: 2014 "Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik", **Resmi Gazete,** (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2014/07/20140711-5.htm, 13 Mart 2023

Resmi Gazete: 2021 "Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik", **Resmi Gazete,** (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2021/02/20210226-2.htm, 20 Mayıs 2023

Salami, I.: 2020 "COVID-19 Crisis in Africa: Leveraging FinTech and RegTech for Economic Recovery", **Journal of International Banking Law and Regulation,** 35/10, 410, (Çevrimiçi) https://repository.uel.ac.uk/item/887qw, 27 Mayıs 2023

Sanction Scanner, t.y.(a) "About Us", **Sanction Scanner,** (Çevrimiçi) https://sanctionscanner.com/about-us, 28 Mayıs 2023

Sanction Scanner, t.y.(b) "Sanction Scanner Ranked 8th in Deloitte Fast50", **Sanction Scanner** (Çevrimiçi) https://sanctionscanner.com/blog/sanction-scanner-selected-as-8th-company-in-deloitte-technology-fast50-692, 28 Mayıs 2023

Sanction Scanner, t.y.(c) "Sanction Scanner is Named a Regtech100 Company", **Sanction Scanner** (Çevrimiçi) https://sanctionscanner.com/blog/sanction-scanner-is-named-a-RegTech100-company-681, 28 Mayıs 2023

Sanction Scanner: 2022 "2022 Türkiye AML Yıllık Raporu", **Sanction Scanner,** (Çevrimiçi) https://lp.sanctionscanner.com/2022-t%C3%BCrkiye-aml-y%C4%B1ll%C4%B1k-raporu, 28 Mayıs 2023

Santomero, A. M.: 1997 "Commercial Bank Risk Management: An Analysis of the Process", **Journal of Financial Services Research**, Kluwer Academic Publishers, 12, 88 (Çevrimiçi) https://link.springer.com/article/10.1023/A:1007971801810, 28 Mayıs 2023

Sarac, A.: 2020 "Challenger Banking Kavramı ve Gelişimi", **Fintechtime** (Çevrimiçi) https://fintechtime.com/tr/2020/02/challenger-banking-kavrami-ve-gelisimi/, 28 Mayıs 2023

Saucier, D., 2022 "4 Big Challenges to RegTech Success for Financial Services Firms", **Purestorage** (Çevrimiçi) https://blog.purestorage.com/solutions/4-big-challenges-to-regtech-success-for-financial-services-firms/, 27 Mayıs 2023

Scott, B. F.: 2019 "Halkbank and OFAC: a sanctions evasion case study", **Journal of Money Laundering Control**, 22/4, 734-743 (Çevrimiçi) https://doi.org/10.1108/JMLC-12-2018-0074, 29 Mayıs 2023

SEC: 2017 "Wells Fargo Board Releases Findings Of Independent Investigation Of Retail Banking Sales Practices And Related Matters", **SEC**, 13-79 (Çevrimiçi) https://www.sec.gov/Archives/edgar/data/72971/000119312517118654/d375947ddefa14a.htm, 28 Mayıs 2023

SEC: 2021 "JPMorgan Admits to Widespread Recordkeeping Failures and Agrees to Pay $125 Million Penalty to Resolve SEC Charges", **SEC** (Çevrimiçi) https://www.sec.gov/news/press-release/2021-262, 28 Mayıs 2023

Singh, C., Lin, W.: 2020 "Can artificial intelligence, RegTech and CharityTech provide effective solutions for anti-money laundering and counter-terror financing initiatives in charitable fundraising", **Journal of Money Laundering Control**, 474-476 (Çevrimiçi) https://doi.org/10.1108/JMLC-09-2020-0100, 27 Mayıs 2023

Sözcü: 2020 "BDDK'dan bankalara iki ayda 326 milyon TL para cezası", **Sözcü** (Çevrimiçi) https://www.sozcu.com.tr/2020/ekonomi/bddkdan-bankalara-iki-ayda-326-milyon-tl-para-cezasi-5922655/ü 28 Mayıs 2023

Statistica: 2023 "Cumulative number of European Union (EU) sanctions against Russian individuals and entities over the territorial integrity of Ukraine from March 2014 to April 2023", **Statistica**, (Çevrimiçi) https://www.statista.com/statistics/1293589/eu-sanctions-against-russia/, 28 Mayıs 2023

Şahin, B. Ş., Cantürk, B. C.: 2020 "Türkiye'deki Hukuki Altyapı ve Ödeme Hizmetleri Yönergesi 2 Bağlamında API Teknolojisi ve Açık Bankacılık." **Maliye ve Finans Yazıları,** 114, 149-180 (Çevrimiçi) https://dergipark.org.tr/en/download/article-file/838825, 28 Mayıs 2023

Tayan, B.: 2019 "The Wells Fargo cross-selling scandal", **Rock Center for Corporate Governance at Stanford University Closer Look Series: Topics, Issues and Controversies in Corporate Governance No. CGRP-62 Version,** 2, 17-1, (Çevrimiçi) https://corpgov.law.harvard.edu/2019/02/06/the-wells-fargo-cross-selling-scandal-2/, 28 Mayıs 2023

TBB, t.y. "Düzenlemeler", **TBB** (Çevrimiçi) https://www.tbb.org.tr/tr/bankacilik/duzenlemeler/5, 20 Mayıs 2023

TBB-MASAK Çalışma Grubu: 2005 "Suç Gelirlerinin Aklanması ve Terörizmin Finansmanı ile Mücadelenin Önemi: Türk Bankacılık Sisteminde İyi Uygulama Kılavuzu", **Bankacılar Dergisi,** 54, 87-94 (Çevrimiçi) https://www.tbb.org.tr/Dosyalar/Arastirma_ve_Raporlar/KaraparaTBBKlavuz_Eylul2005.pdf, 10 Mart 2023

TBB-MASAK Çalışma Grubu: 2007 "Para Aklama Riskinin Yönetimi ve Türk Bankacılık Sisteminde Uygulama Kılavuzu", **Bankacılar Dergisi**, 60, 58-66, (Çevrimiçi) https://www.tbb.org.tr/Dosyalar/Arastirma_ve_Raporlar/para_aklama_riskinin_yonetimi.pdf, 24 Şubat 2023

TDK (Çevrimiçi) https://sozluk.gov.tr/, 10 Nisan 2023

Teeter, R. A., Alles, M. G., Vasarhelyi, M. A.: 2010 "The Remote Audit", **Journal of Emerging Technologies in Accounting**, 7/1, 73-88 (Çevrimiçi) https://doi.org/10.2308/jeta.2010.7.1.73, 29 Mayıs 2023

Tepe, B., Ardıyok, Ş.: 2004 "Devlete yeni rol: Regülasyon", **Amme İdaresi Dergisi,** 37/1, 10-130

Thomson Reuters: 2018 "Cost Of Compliance 2018", **Thomson Reuters,** 1-38 (Çevrimiçi) https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/cost-of-compliance-special-report-2018.pdf, 28 Mayıs 2023

Thornhill, W. T.: 1981 "Complete Handbook of Operational and Management Auditing", **Prentice Hall,** USA,

Tiryaki, G.: 2010 "Bankacılık Sektöründe -Basel Sermaye Uzlaşıları- Sermaye Yeterliliği Standart Rasyosu Gerçekten Yeterli Midir? Kaldıraç Oranı'na ve Daha Güçlü Bir Bankacılık Düzenleme Çerçevesine İlişkin Değerlendirmeler", **Vergi Dünyası Dergisi**, 347. Sayı, Temmuz 2010, 118-122

Toronto Centre: 2017 "FinTech, RegTech and SupTech: What they mean for financial supervision", **Toronto Centre Notes,** 1-18 (Çevrimiçi) https://www.torontocentre.org/videos/FinTech_RegTech_and_SupTech_What_They_Mean_for_Financial_Supervision.pdf, 28 Mayıs 2023

Tyagi, N.: 2021 "What is RegTech? Requirement & Benefits", **Analyticsteps** (Çevrimiçi) https://www.analyticssteps.com/blogs/what-regtech-requirement-benefits, 27 Mayıs 2023

U.S. District Court-Southern District of New York: 2017 "Superseding Indictment - United States of America vs Reza Zarrab et al", **U.S. District Court - Southern District of New York**, 16-26 (Çevrimiçi) https://www.justice.gov/usao-sdny/press-release/file/994976/download, 29 Mayıs 2023

U.S. District Court-Southern District of New York: 2018 "Decision and Order - Unıted States Of Amerıca, Government. vs. Mehmet Hakan Atilla, Defendant", **U.S. District Court - Southern District of New York,** (Çevrimiçi) https://casetext.com/case/united-states-v-atilla, 29 Mayıs 2023

Uipath, t.y. "Robotic Process Automation (RPA): Automation software to end repetitive tasks and make digital transformation a reality", **Uipath,** (Çevrimiçi) https://www.uipath.com/rpa/robotic-process-automation#:~:text=Robotic%20process%20automation%20(RPA)%20is,with%20digital%20systems%20and%20software, 28 Mayıs 2023

Uzunoğlu, E., t.y. "RegTech Bağımsızlığını İlan Etmeli!", **Cube incubation**, (Çevrimiçi) https://www.cubeincubation.com/blog/RegTech-bagimsizligini-ilan-etmeli, 28 Mayıs 2023

Üstün, O.: 2016 "Açıklamalı İngilizce - Türkçe Kara Para Terimleri Ve Kavramları Sözlüğü", **Türkiye Bankalar Birliği**, 3. Baskı, İstanbul, 2016, 4

Violation Tracker: 2023 "Wells Fargo", **Violation Tracker,** (Çevrimiçi) https://violationtracker.goodjobsfirst.org/?parent=wells-fargo&order=company&sort=, 28 Mayıs 2023

Vivek, D., Rakesh, S., Walimbe, R. S., Mohanty, A.: 2020 "The Role of CLOUD in FinTech and RegTech", **Annals of the University Dunarea de Jos of Galati Fascicle I, Economics & Applied Informatics,** 26/3, 10, (Çevrimiçi) https://www.researchgate.net/publication/348164459_The_Role_of_CLOUD_in_FinTech_and_RegTech, 27 Mayıs 2023

Von Solms, J.: 2021 "Integrating Regulatory Technology (RegTech) into the digital transformation of a bank Treasury", **Journal of Banking Regulation**, 22/2, 152-196 (Çevrimiçi) https://link.springer.com/article/10.1057/s41261-020-00134-0, 27 Mayıs 2023

Wall, L. D.: 2018 "Some financial regulatory implications of AI", **JEB**, 100, 55-63 (Çevrimiçi) https://doi.org/10.1016/j.jeconbus.2018.05.003, 27 Mayıs 2023

WEF: 2018 "The new physics of financial services", **WEF** (Çevrimiçi) https://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf, 27 Mayıs 2023

Wells Fargo, t.y. "History of Wells Fargo", **Wells Fargo,** (Çevrimiçi) https://www.wellsfargo.com/about/corporate/history/, 28 Mayıs 2023

Wells Fargo: 2017 "2017 Performance Management & Rewards Summary of New Program", **Wells Fargo Media**, (Çevrimiçi) https://www08.wellsfargomedia.com/assets/pdf/commitment/performance.pdf, 28 Mayıs 2023

Wells Fargo: 2022 "Wells Fargo 2022 Annual Report", **Wells Fargo Media** (Çevrimiçi) https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/annual-reports/2022-annual-report.pdf, 28 Mayıs 2023

Williams, J.: 2018 "How Artificial Intelligence Can Help Mend the UK's Broken Audit System", **The Fintech Times**, (Çevrimiçi) https://thefintechtimes.com/artificial-intelligence-audits/, 29 Mayıs 2023

Wilson, H.: 2021 "StanChart Hit With $61 Million Fine After Spreadsheet Error", **Bloomberg,** (Çevrimiçi) https://www.bloomberg.com/news/articles/2021-12-20/bank-of-england-fines-stanchart-61-million-for-reporting-lapses, 26 Mayıs 2023

Witman, P. D.: 2018 "Teaching Case 'What gets measured, gets managed' the wells fargo account opening scandal", **Journal of Information Systems Education**, 29/3, 132-136, (Çevrimiçi) https://www.researchgate.net/publication/328718957_What_Gets_Measured_Gets_Managed_-_The_Wells_Fargo_Account_Opening_Scandal, 28 Mayıs 2023

Witten, I. H., Frank, E.: 2005 "Data Minig Practical Machine Learning Tools and Techniques", **Morgan Kaufmann Publishers**, 2. Baskı, San Francisco, xxiii (Çevrimiçi) http://academia.dk/BiologiskAntropologi/Epidemiologi/DataMining/Witten_and_Frank_DataMining_Weka_2nd_Ed_2005.pdf, 28 Mayıs 2023

Wright, M.: 2019 "Can AI Disrupt Monitoring for Suspicious Activity?", **The REGTECH Book, John Wiley & Sons**., s.231-235

Yang, D., Li, M.: 2018 "Evolutionary approaches and the construction of technology-driven regulations", **Emerging Markets Finance and Trade**, 54/14, 3256-3271

Zhu, S.: 2021 "Audit and technology", **2021 3rd International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI),** 745-749, (Çevrimiçi) https://doi.org/10.1109/MLBDBI54094.2021.00145, 29 Mayıs 2023

Zoet, M., Welke, R., Versendaal, J., Ravesteyn, P.: 2009 "Aligning Risk Management and Compliance Considerations with Business Process Development", **E-Commerce and Web Technologies: 10th International Conference,** EC-Web 2009, Springer Berlin Heidelberg, 157-168