



T I
ACADEMIA
R e s e a r c h
Governance, Risk, Control & Audit

Volume/Cilt: 3 - Issue/Sayı: 1-January-July/Ocak-Temmuz 2021



Türkiye İç Denetim Enstitüsü
The Institute of Internal Auditing - Turkey

TİDE

AcademIA

R e s e a r c h

GOVERNANCE, RISK, CONTROL & AUDIT

Volume/Cilt: 3 - Issue/Sayı: 1-January-July/Ocak-Temmuz 2021

Print ISSN: 2667-5412
Published in English & Turkish

TİDE Academia Research

TİDE ACADEMIA Research, Governace, Risk, Control & Audit

Volume/Cilt: 3 - Issue/Sayı: 1- January-July/Ocak-Temmuz 2021

Biannual Peer - Reviewed Academic Journal / 6 Aylık Hakemli Akademik Dergi

Print ISSN: 2667-5412

Owner / Türkiye İç Denetim Enstitüsü Adına İmtiyaz Sahibi

Ali Kamil Uzun

Responsible Desk Editor / Sorumlu Yazı İşleri Müdürü

Prof. Dr. Dursun Arıkboğa

Editor in Chief / Editör

Prof. Dr. Nuran Cömert

Assistant Editors / Editör Yardımcıları

Arş. Gör. Dr. Nevzat Güngör

Arş. Gör. Dr. Ömer Faruk Tan

Arş. Gör. Sezer Külâh

Editorial Board / Yayın Kurulu

Prof. Dr. Nuran Cömert

Ali Kamil Uzun

Prof. Dr. Dursun Arıkboğa

Tolga Usluer

Ethem Yenigün

Gürdoğan Yurtsever

Print Editor / Yayına Hazırlama Sorumlusu

Serpil Kaya Vurgun

E-posta: serpil.vurgun@gmail.com

Contact / Dergi İletişim

E-mail: academia@tide.org.tr

Phone: 0212 212 55 24-25

Address: Mecidiyeköy Mah. Cemal Sahir Sokak No : 29 D:30-31 Şişli – İstanbul - Turkey

TIDE AcademIA Research is a scientific peer-reviewed journal which is going to be published twice in a year (July-December) by the Institute of Internal Auditors – Turkey (TIDE). An essential objective of the journal is to promote communication between research and practice, which will influence present and future developments in governance, risk, control and auditing education as well as research and practice. The language of the journal is Turkish and English.

TİDE AcademIA Research Dergisi, Türkiye İç Denetim Enstitüsü (TİDE) tarafından yılda iki kez (Temmuz-Aralık) yayımlanan bilimsel hakemli bir dergidir. Derginin temel amacı, bugün ve gelecekteki kurumsal yönetim, risk yönetimi, kontrol ve denetim ile ilgili konularda teori ve uygulamayı geliştirmeye katkı sağlayacak özgün ve yeni bilimsel çalışmalar yayınlamak ve böylece uygulamacı ve araştırmacılar arasında iletişimi artırmaktır. Derginin yazım dili Türkçe ve İngilizcedir.



Advisory Board / Danışma Kurulu

- Tonya D. Baez, *CIA (IIA-ARC)*
Gudmundur I. Bergthorsson (*IIA*)
Laurent Philippe Berliner, *CIA, CRMA (IIA-ARC)*
Marianne Breccia, *CRMA (IIA-ARC)*
Stuart W. Campbell, *CIA, CGAP (IIA-ARC)*
Philip Andrew Draber, *CIA, CRMA (IIA-ARC)*
Hossam Hosni Abdelaziz Elshaffei (*IIA*)
Prof. Dr. Melih Erdoğan
Prof. Dr. Lerzan Kavut
Prof. Dr. İdil Kaya
Prof. Dr. Ömer Lalik
Prof. Dr. Beyhan Marşap
Paul C. Kiley, *CIA (IIA-ARC)*
James Molzahn (*IIA*)
Prof. Dr. Nur İrem Nuhoglu (*PhD*) (*IIA-ARC*)
Sandra L. Pundmann (*IIA*)
Mark L. Salamasick, *CIA, CRMA (IIA-ARC)*
Dominique Vincenti (*IIA*)

Referee Board / Hakem Kurulu

- Prof. Dr. Nalan Akdoğan - *Başkent University, TURKEY*
Prof. Dr. Nesrin Alptekin - *Anadolu University, TURKEY*
Prof. Dr. Ümmühan Aslan - *Bilecik Şeyh Edebali University, TURKEY*
Prof. Dr. Emin Avcı - *Marmara University, TURKEY*
Prof. Dr. Çağnur Kaytmaz Balsarı - *Dokuz Eylül University, TURKEY*
Rudrik du Bruyn, *CIA (IIA-ARC) - University of Pretoria, SOUTH AFRICA*
Prof. Dr. Ahmet Vecdi Can - *Sakarya University, TURKEY*
Prof. Dr. Fatih Dalkılıç, *CIA - Dokuz Eylül University, TURKEY*
Prof. Dr. Ali Deran - *Tarsus University, TURKEY*
Prof. Dr. Volkan Demir - *Galatasaray University, TURKEY*
Prof. Dr. Nurten Erdoğan - *Anadolu University, TURKEY*



- Prof. Dr. Melih Erdoğan - *Anadolu University, TURKEY*
Prof. Dr. Mert Erer - *Marmara University, TURKEY*
Assoc. Prof. Dr. Graham Gal - *University of Massachusetts, USA*
Jean Pierre Garitte - *University of Antwerp, Management School, BELGIUM*
Prof. Dr. Cemal İbiş - *Işık University, TURKEY*
Prof. Dr. Selahattin Karabınar - *İstanbul University, TURKEY*
Prof. Dr. Lerzan Kavut - *İstanbul University, TURKEY*
Prof. Dr. İdil Kaya - *Galatasaray University, TURKEY*
Prof. Dr. Ganite Kurt - *Ankara Hacı Bayram Veli University, TURKEY*
Prof. Dr. Tamer Koçel - *Kültür University, TURKEY*
Assoc. Prof. Dr. Ufuk Mısırlıoğlu - *University of the West of England, UK*
Prof. Dr. Nur İrem Nuhoglu - *Boğaziçi University, TURKEY*
Prof. Dr. Helmut Pernsteiner - *Johannes Kepler University, AUSTRIA*
Prof. Dr. Yakup Selvi - *İstanbul University, TURKEY*
Alan N. Siegfried, *CIA, CCSA, CFSA, CGAP, CRMA - University of Maryland, USA*
Jared Scott Solleau, *CIA, CCSA, CRMA - Louisiana State University, USA*
Prof. Dr. Süleyman Uyar - *Alanya Alaaddin Keykubat University, TURKEY*
Prof. Dr. Saime Önce - *Anadolu University, TURKEY*
Dr. Chung Fern Wu - *National Taiwan University, TAIWAN*
Prof. Dr. Birol Yıldız - *Osmangazi University, TURKEY*
Prof. Dr. Fatih Yılmaz - *İstanbul University, TURKEY*
Prof. Dr. Serra Yurtkoru - *Marmara University, TURKEY*
Prof. Dr. Göksel Yücel - *Türk-Alman University, TURKEY*
Prof. Dr. Çağla Ersen Cömert - *Marmara University, TURKEY*
Prof. Dr. Banu Tarhan Mengi - *Marmara University, TURKEY*
Adjunct Prof. Dr. Aslı Yüksel Mermod - *Webster University, SWITZERLAND*
Prof. Dr. Fatma Ulucan Özkul - *Bahçeşehir University, TURKEY*
Prof. Dr. Esin Can - *Yıldız Teknik University, TURKEY*
Prof. Dr. N. Aylin Ataay Saybaşı - *Galatasaray University, TURKEY*
Prof. Dr. Dilek Zamantılı Nayır - *Türk-Alman Üniversitesi, TURKEY*
Prof. Dr. İrem Eren Erdoğan - *Marmara Üniversitesi, TURKEY*
Prof. Dr. İdil Koç - *Marmara Üniversitesi, TURKEY*

Contents / İindekiler

Preface / Sunuř	8
Türk Bankacılık Sektörünün İ Sistemlerine Eleřtirel Bir Yaklařım / <i>A Critical Approach to the Internal Systems of the Turkish Banking Sector</i>	
Yağızcan Yücel ENDİK, Duygu ANIL KESKİN	11
Muhasebe ve Denetimde Mesleki Yargının Epistemolojik Boyutu: Özne-Nesne İliřkisi/ <i>Epistemological Dimensions of Professional Judgment in Accounting and Auditing: Subject-Object Relationship</i>	
Selahattin KARABINAR	41
Using Big Data in Internal Fraud Detection / <i>İ Suiistimalin Tespitinde Büyük Verinin Kullanılması</i>	
Teoman Samet TEMUİN, Sefa ERBAŐ, Anıl AY	55
Covid-19 Krizinde Sürdürülebilirlik Performansı ve Anormal Pay Getirisi Etkileri / <i>Sustainability Performance and Abnormal Stock Returns During the Covid-19 Crises</i>	
Emrah KELEŐ	83
The External Financial Statement Audit Process and Blockchain Technology / <i>Finansal Tabloların Bağımsız Denetim Süreci ve Blokzincir Teknolojisi</i>	
Graham GAL, Matthew SHERWOOD	103
Formatting Guide	141

Preface

Dear Esteemed Readers,

In this issue of the TİDE Academia Research, we present you five interesting theoretical and empirical research and review articles directly or indirectly related to auditing, internal control and governance.

We hope the articles, which went through rigorous referee reviews, will contribute to the literature and practice. Wishing you pleasant readings until we meet again in our next issue.

Faithfully yours,

Prof. Nuran Cömert (PhD)
Editor in Chief

Sunuş

Merhabalar Değerli Okurlarımız,

TİDE Academia Research'ün bu sayısında sizlere denetim, iç kontrol ve yönetimle doğrudan ve dolaylı ilgisi olan ilginizi çekecek beş teorik ve amprik araştırma ve inceleme makalesi sunuyoruz.

Titiz hakem değerlendirmesi sürecinden geçen makalelerin literatüre ve uygulamaya önemli katkı sağlayacağını umuyor gelecek sayımızda tekrar buluşmak üzere keyifli okumalar diliyoruz.

Prof. Dr. Nuran CÖMERT
Editör

Research Article/Araştırma Makalesi

TÜRK BANKACILIK SEKTÖRÜNÜN İÇ SİSTEMLERİNE ELEŞTİREL BİR YAKLAŞIM

Yağızcan Yücel ÇENDİK¹Duygu ANIL KESKİN²

Submitted/Başvuru: 15.06.2021

Last Revised/Son Düzeltme: 06.07.2021

Accepted/Kabul: 09.07.2021

Öz

Ekonominin düzenleyici kurumlarından biri olan bankalar, tabiatları gereği sıklıkla riske maruz kalmaktadırlar. Maruz kaldıkları risklere karşılık vermeye yönelik geçmişten günümüze çeşitli yaklaşımlar benimsenmekle birlikte artan küreselleşme, gelişen teknoloji, farklılaşan hizmet şekilleri ve derinleşen finansal piyasa koşulları risklerin çeşit ve boyutlarını arttırmıştır. Bu kapsamda geleneksel risk yönetimi sürecinin etkinliği açısından iç denetim faaliyetinin tek başına yeterliliği sorgulanmaya başlanmıştır. Bankacılıkta karşılaşılan çok farklı sayıda ve türdeki yeni riskler, kurumun iç sistemlerinin etkinliğinin önemini giderek arttırmaktadır. Her ne kadar Dünya'da yaygın uygulama bankaların denetiminin kamu otoriteleri, bağımsız denetim kuruluşları ve bankaların kendi iç denetim birimleri aracılığıyla denetlenmesi şeklindeyse de özellikle son 20 yıldır iç sistemlerin kurulmasının önemi artmaya başlamıştır. Giderek artan sayıda banka, karşılaşılan risklerin minimize edilmesi için belirlenen politika ve prosedürlerden oluşan, geleneksel denetim fonksiyonunun yanı sıra yönetim ve çalışanların da dahil olduğu bir iç kontrol sistemini oluşturmuş-

1 Sorumlu Yazar, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme (İktisat) Doktora Programı, yagizcancendik@gmail.com, ORCID: 0000-0003-2562-3987

2 Doç. Dr., İstanbul Üniversitesi, İktisat Fakültesi, İşletme Bölümü, danil@istanbul.edu.tr, ORCID: 0000-0003-3069-0615

To cite this article: Çendik, Y. Y., & Anıl-Keskin, D. (2021). Türk Bankacılık Sektörünün İç Sistemlerine Eleştirel Bir Yaklaşım. *TİDE Academia Research*, 3(1), 11-40

lardır. Günümüzde iç kontrolün tanımı neredeyse bütün uluslararası otoritelerce benzer şekilde yapılsa da uygulamada farklılıklar görülmektedir. Türkiye’de ise kontrol ve denetim sıklıkla birbirleri yerine kullanılan kavramlar olarak karşımıza çıkmaktadır.

Anahtar Kelimeler: İç Denetim, İç Kontrol, Üçlü Savunma Hattı, Çevik Denetim, Bankacılık

JEL Sınıflandırması: G21, M40, M42

A CRITICAL APPROACH TO THE INTERNAL SYSTEMS OF THE TURKISH BANKING SECTOR

Abstract

As one of the regulating institutions of the economy, banks are often exposed to risk due to their nature. While various approaches have been adopted from past to present to respond to the risks they are exposed to, increasing globalization, developing technology, differentiating service forms and deepening financial market conditions have increased the types and dimensions of risks. In this context, the adequacy of the internal audit activity alone has begun to be questioned in terms of the effectiveness of the traditional risk management process. The many different types and numbers of new risks encountered in banking are increasing the importance of the efficiency of the internal systems of the institution.

Although the common practice in the world is the supervision of banks by public authorities, independent audit institutions and their own internal audit units, the importance of establishing internal systems has started to increase especially in the last 20 years. An increasing number of banks have established an internal control system that includes management and employees, as well as the traditional audit function, which consists of policies and procedures determined to minimize the risks encountered.

Today, although the definition of internal control is made similarly by almost all international authorities, there are differences in practice. In Turkey, on the other hand, control and auditing are frequently used interchangeably.

Keywords: Internal Audit, Internal Control, Three Lines of Defence, Agile Audit, Banking

JEL Classification: G21, M40, M42

Extended Summary

As one of the regulating institutions of the economy, banks are often exposed to risk due to their nature. While various approaches have been adopted from past to present to respond to the risks they are exposed to, increasing globalization, developing technology, differentiating service forms and deepening financial market conditions have increased the types and dimensions of risks. In this context, the adequacy of the internal audit activity alone has begun to be questioned in terms of the effectiveness of the traditional risk management process. The many different types and numbers of new risks encountered in banking are increasing the importance of the efficiency of the internal systems of the institution.

Today, although the definition of internal control is made similarly by almost all international authorities, there are differences in practice. In Turkey, on the other hand, control and auditing are frequently used interchangeably.

Introduction

The banking sector is an integral part of the modern financial structure due to its auxiliary role in economic policy implementations and its intermediary role in domestic and foreign trade. The key role of banks in financial stability has necessitated the regulation of the banking system both at national and international level. Because historical experiences show that a crisis that emerges in the banking sector spreads to different sectors, both nationally and internationally, with its spillover effect.

Audits carried out to evaluate the adequacy of banks in responding to the risks they are exposed to and the effectiveness of their processes generally come in three forms. The first of these is the supervision of banks by public authorities. Within the framework of the Basel Committee decisions, the Banking Regulation and Supervision Agency was established in Turkey and the transactions of banks were subject to the supervision of this institution. Another supervision mechanism is the supervision of banks through independent audit institutions. The audit performed by independent audit firms mostly covers financial statements, but is not limited to this. Third and lastly, there are internal audit units established within the banks themselves.

In this study, since the functioning of the concept of internal audit and internal control in the banking sector in practice will be examined, the audits carried out by the independent audit institutions and public authorities are not mentioned. In this context, firstly internal audit and then internal control will be examined conceptually and its applications in Turkish banks will be tried to be included.

Literature Review

When the International Institute of Internal Auditors reports, American legislation, European Union legislation, Basel Committee reports and Turkish banking legislation are examined, it is understood that the internal audit units of the banks established to add value to its activities. Internal audit has to provide an independent and objective assurance, and has to report directly to the board of directors in order to not to be affected by the company managers, and its has to cover all business and transactions.

The technological developments in the world, the changing business environment and the differentiation of banking services require internal audit units to keep up with the times and renew themselves. Experiences in the past years have increased the expectations of stakeholders for a more effective assurance and risk management. In this new business environment, internal audit should respond rapidly to emerging changes, develop a more risk-based audit approach, modernize working papers, and increase its expertise, especially in areas of increasing importance, such as cybercrime.

Even in the early 1900s, when modern internal control approaches did not emerge, control was defined as a management function. Fayol identified control as one of the 5 basic elements of management. According to him, control is “watching that everything is in accordance with the given orders and existing rules.” (Sengul, 2007). Internal audit, on the other hand, is designed separately from the management in accordance with the principles of independence and objectivity. Internal audit is not responsible for the negative effects that arise as a result of not taking adequate or effective actions against the risks faced by banks, unless there is a significant audit error. The fact that the responsibility for these negative effects is only on the senior management and / or the relevant personnel who give place to the deficiencies has led to the need to put forward a risk management model

that includes management, employees and all stakeholders in order to prevent these deficiencies and mistakes.

The developments experienced in the international banking sector in the past years make it necessary to assign duties and responsibilities to the bank managements and the business as a whole in order to manage the risks, as well as the independent internal audit activities. In this context, the importance of the internal control system that banks will establish within their own structures is increasing.

While internal audit emerges as an independent structure, internal control is defined as a process that is affected by the board of directors, management and employees from all levels. From this point of view, internal control is a system that should be established by top managers under the responsibility of the board of directors to manage accepted risks. This responsible approach to risk management includes not only detecting incomplete or faulty transactions, but also preventing deficiencies and errors before they occur.

Conclusion

When the integrated annual reports of the banks are examined, it is seen that the internal control unit is in charge of helping the bank's activities to be carried out in accordance with the internal and external legislation. However, in Turkish banking practice, internal control units are not involved in the management's policy and procedure formulation process, including self-assessment. Instead of taking part in the process of establishing internal control, policies and procedures, it acts as an audit function, audits the compliance of policies and procedures with internal and external legislation, and carries out an audit that reports any deficiencies to the board of directors and senior management. One way to prevent the dual audit mechanism in Turkey is to include the internal control mechanism in the process of establishing policies and procedures in line with international examples. The task of internal audit should be to supervise the effectiveness and efficiency of policies and procedures in line with internal and external legislation. This approach will be compatible with the "Three Lines of Defense" model proposed by COSO and the International Institute of Internal Auditors.

The internal audit units of banks will be able to provide services in a more specialized area with fewer employees, thanks to the loss of importance of labor-intensive audits and the rapid and short-term on-site audits to be carried out only when needed, with an agile audit approach. An agile internal audit unit that will perform audits when needed to deal with shape-shifting risks and a widespread internal control system established by management to support this will both reduce risk management costs and prevent duplication of effort.

1. Giriş

Bankacılık sektörü, gerek ekonomi politikası uygulamalarındaki yardımcı rolü gerekse iç ve dış ticarete aracı rolü sebebiyle, modern finansal yapının ayrılmaz bir parçasıdır. Bankaların finansal istikrar üzerindeki kilit rolü, bankacılık sisteminin hem ulusal hem uluslararası düzeyde regüle edilmesi gerekliliğini doğurmuştur. Çünkü tarihsel deneyimler göstermektedir ki bankacılık sektöründe ortaya çıkan bir kriz, yayılma etkisi ile hem ulusal hem de uluslararası farklı sektörlere sıçramaktadır.

Yapılan çalışmalarda Japon bankalarından kaynaklanan bir finansal krizin, Amerikan reel sektörü üzerinde olumsuz etkileri olduğu ortaya koyulmuştur. (Peek & Rosengren,2000) Bankalar karşı karşıya kaldıkları sistemik riskleri, bankalar arası piyasalardaki borç-alacak ilişkisi ve ödeme sistemleri aracılığıyla diğer bankalara ve ülkelere ihraç etme eğilimindedir. (Kaufman &Scott, 2003) Bir ülkede yaşanan bankacılık krizinin hem o ülkedeki finans dışı sektörler hem de diğer ülkeler ve uluslararası finansal sistemler üzerindeki yayılma etkisinin anlaşılması ve 1970’li yılların başında yaşanan uluslararası bankacılık krizi, bankaların uluslararası bir kurum tarafından regüle edilmesi ihtiyacını doğurmuştur. Bu ihtiyaç doğrultusunda, on ülkenin merkez bankası başkanları öncülüğünde, uluslararası bankacılık sisteminin regüle edilmesine yönelik çalışmalar yapılmış ve bu çalışmaların sonucunda 1974 yılının sonunda Basel Komitesi kurulmuştur.

Kurulan bu komite, çoğunlukla bankaların sermaye yapısının güçlendirilmesi alanında çalışmalar yapmışsa da bankaların kurumsal yönetim uygulamalarının, karşılaşılan risklerin yönetilmesinde çok büyük bir öneme sahip olduğunun anlaşılmasıyla birlikte bankaların kurumsal yönetim ilkeleri hakkında da bir takım ilke ve prosedürler açıklamaya başlamıştır. Bu çerçevede Basel Komitesi, yönetim kurulunun sorumlulukları ve yetkinliği, üst yönetimin görevleri, risk yönetimi fonksiyonunun yapısı, uyum riskinin yönetilmesi, iç denetimin etkin bir yönetim süreci içerisindeki uzun dönemli rolü, ücret yönetimi, yönetim ve raporlamada açıklık konularını kapsayan on üç adet ilke öngörmüştür. (Basel Komitesi, 2015)

Bankaların maruz kaldıkları risklere cevap vermedeki yeterliliğini ve süreçlerinin etkinliğini değerlendirmek üzere gerçekleştirilen denetim çalışmaları genel olarak üç şekilde karşı-

mıza çıkmaktadır. Bunlardan ilki bankaların kamu otoriteleri vasıtasıyla denetlenmesidir. Basel Komitesi kararları çerçevesinde Türkiye’de de Bankacılık Düzenleme ve Denetleme Kurumu kurulmuş ve bankaların yaptıkları iş ve işlemler bu kurumun gözetimine tabi tutulmuştur. Bir diğer denetim mekanizması, bankaların bağımsız denetim kuruluşları vasıtasıyla denetlenmesidir. Bağımsız denetim kuruluşlarının gerçekleştirdiği denetim daha çok finansal tabloları kapsamakla birlikte yalnızca bununla sınırlı değildir. Üçüncü ve son olarak ise bankaların kendi bünyelerinde kurulmuş olan iç denetim birimleri bulunmaktadır.

Bu çalışmada, bankacılık sektöründe iç denetim ve iç kontrol kavramının uygulamadaki işleyişi irdeleneceği için bağımsız denetim ve kamu otoritesi vasıtasıyla yapılan denetim çalışmalarına değinilmemiştir. Bu kapsamda öncelikle iç denetim, daha sonra ise iç kontrol kavramsal açıdan incelenecek ve Türk bankalarındaki uygulamalarına yer verilmeye çalışılacaktır.

2. Bankalarda İç Denetim Yaklaşımı

Bankaların maruz kaldıkları risklerin yönetilmesinde en önemli araç, bankaların kendi bünyelerinde oluşturdukları geleneksel iç denetim birimleridir. İç denetim, Uluslararası İç Denetçiler Enstitüsü tarafından “Bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyeti” olarak tanımlanmaktadır. Uluslararası kabul görmüş olan bu tanımdan da anlaşılacağı üzere iç denetim, her ne kadar kurum bünyesinde oluşturulan bir faaliyet olsa da bağımsızlığını ve objektifliğini koruyarak işletmeye değer katmaya çalışan bir süreçtir. İç denetimin kurum bünyesinde kurulan bir faaliyet olması bazı sorunları beraberinde getirmektedir. Geniş çerçevede tartışılan önemli bir sorun, bir kuruma bağlı denetim personelinin, o kurumun çıkarını gözetip gözetmeyeceği, yani bağımsızlık ve objektiflik ilkelerinin zedelenip zedelenmeyeceğidir.

Bu sorunun çözümüne ilişkin olarak Uluslararası İç Denetçiler Enstitüsü’nün yayınladığı ve uluslararası kabul gören “Uluslararası Mesleki Uygulama Çerçevesi”nde iç denetim yöneticisinin işlevsel olarak doğrudan yönetim kuruluna ve idari olarak da genel müdüre bağlı olmasını tavsiye etmektedir. Genel müdüre olan bu idari bağlılık, iç denetim faaliyeti-

tinin bağımsızlığını ve objektifliğini etkilememektedir. İç denetim yöneticisinin yönetim kuruluna işlevsel olarak bağlı olması, doğrudan iletişim ve etkileşim için bir zorunluluktur. Ayrıca iç denetim, iç kontrollerin etkinlik ve verimliliğini değerlendirerek sistemin mevcut etkinliğine ilişkin güvence vermekte ve iyileştirilmesine ilişkin belirlenecek politika ve prosedürlere yönelik danışmanlık rolüyle kurumun etkin kontrollere sahip olmasına yardımcı olmaktadır.

Uluslararası İç Denetçiler Enstitüsünün yapmış olduğu bu tanımı aynen kabul eden Basel Komitesi iç denetimi, yönetim kuruluna bağımsız bir güvence sağlayan ve bununla birlikte bankanın etkili bir yönetim süreci ve uzun vadeli verimliliğinin sağlanmasına yönelik olarak yönetim kurulu ve üst yönetime destek olan bir faaliyet olarak tanımlanmaktadır. (Basel Komitesi, 2015) İç denetim, bu görevlerini yerine getirirken bağımsızlığını korumak için doğrudan yönetim kuruluna bağlı olmalı ve yalnızca yönetim kurulu veya denetim komitesine rapor vermelidir.

Basel Komitesi iç denetimin, bankanın iç kontrol, risk yönetimi ve kurumsal yönetim süreçlerinin etkin olduğuna dair banka yönetim kurulu ve üst yönetime bağımsız bir güvence sağlaması gerektiğini belirtmiştir. (Basel Komitesi, 2012) İç denetim fonksiyonu, bankanın dış kaynaklı aktiviteleri de dahil olmak üzere bütün aktivitelerini kapsamalıdır. Bu kapsamda iç denetim, risk yönetim sisteminin bir şemsiyesi olarak tarif edilmiş ve ayrıca iç kontrol, ve kurumsal yönetim sistemlerini de kapsadığı değerlendirilmiştir.

Yine Basel Komitesi (2002), iç denetim fonksiyonunun asgari görevlerini şu şekilde sıralamıştır:

- İç kontrol sisteminin etkililiği ve verimliliğinin incelenmesi ve değerlendirilmesi,
- Risk yönetimi prosedürleri ve risk değerlendirme metodolojisinin, finansal raporların güvenilirliğinin ve geçerliliğinin, varlıkların korunması ile ilgili araçların, sermaye yeterliliği ölçme sisteminin ve yasal mevzuatlara uyumun gözden geçirilmesi,
- Operasyonların verimliliğinin değerlendirilmesi,
- İşlemlerin ve iç kontrol prosedürlerinin işleyişinin test edilmesi,

- Düzenleyici ve denetleyici kurumlara yapılan raporların güvenilirliğinin ve zamanında yapılıp yapılmadığının denetlenmesi,
- Özel soruşturmaların yürütülmesi,

Amerika'da 1991 yılında kabul edilen ve yürürlüğe giren "Federal Mevduat Sigorta Kurumu Reform Yasası (FDICIA)" iç denetimin finansal kuruluşlardaki yerini ve temel kuruluş ilkelerini ortaya koymaktadır. Bu yasaya göre iç denetim birimi, iç denetçilerin şirket yöneticilerinden etkilenmeyecekleri bir şekilde kurulmalı ve bağımsızlıkları garanti altına alınmalıdır. Bunun için şirketin operasyonel faaliyetlerinde bulunmayan bir yönetici, iç denetim yöneticisi olarak görevlendirilmeli ve yalnızca denetim komitesine rapor vermelidir. (Federal Mevduat Sigorta Kurumu Reform Yasası, 1991) Amerikan Federal Mevduat Sigorta Kurumu (FDIC) tarafından, bankaların uymasını zorunlu tuttuğu "İnceleme Politikalarına İlişkin Risk Yönetimi Kılavuzu"nda iç denetimin, finansal kuruluşların risk yönetimi ve iç kontrol süreçlerine ilişkin olarak sistematik bir güvence sağlaması gerektiği vurgulanmıştır.

Avrupa Merkez Bankasının öncüsü olan ve 1998 yılına kadar faaliyet gösteren Avrupa Para Enstitüsü tarafından yayınlanan ve finansal kuruluşların iç kontrol sistemleri hakkında temel ilkeleri ortaya koyan raporunda iç denetim, iç kontrol sisteminin anahtar elemanlarından biri olarak tanımlanmış ve iç kontrol sisteminin bağımsız bir değerlendirmesini yapmakla görevlendirilmiştir. (Avrupa Para Enstitüsü, 1997)

5411 sayılı Bankacılık Kanunu'nda da bankaların bütün birim, şube ve ortaklıklarını kapsayan bir iç denetim sistemi kurmaları zorunlu tutulmuş ve bu iç denetim faaliyetlerinin banka müfettişleri aracılığıyla yürütüleceği belirtilmiştir. İç denetim biriminin faaliyetleri ve çalışma esaslarına ise Bankacılık Denetleme ve Düzenleme Kurulu (BDDK) tarafından yayınlanan yönetmelik açıklık getirmektedir. Bu yönetmeliğe göre iç denetim birimi, temel olarak, yapacağı dönemsel ve riske dayalı denetimlerde, bankanın iç kontrol, risk yönetimi ve bilgi sistemlerinin yeterliliğini ve etkinliğini değerlendirmekte, gerçekleştirilen işlemlerin iç ve dış mevzuata uygunluğunu denetleyerek, finansal raporların doğruluğunu incelemektedir. (BDDK, 2014)

İç denetimin uzun zamandır bir risk yönetimi aracı olması ve üzerinde çok fazla araştırma yapılmasının da yardımıyla, hemen hemen her ülke ve kurumda benzer tanımlar ve görevler ortaya çıkmıştır. Özetle Uluslararası İç Denetçiler Enstitüsü, Amerikan mevzuatı, Avrupa Birliği mevzuatı, Basel Komitesi Raporları ve Türk bankacılık mevzuatı incelendiğinde, bankaların iç denetim birimlerinin, bütün iş ve işlemleri kapsayacak şekilde, şirket yöneticilerinden etkilenmemek için doğrudan yönetim kuruluna bağlı olarak, bağımsız ve objektif bir güvence sağlamak ve şirket faaliyetlerine değer katmak üzere kurulduğu anlaşılmaktadır.

Dünya’da yaşanan teknolojik gelişmeler, değişen iş çevresi ve bankacılık hizmetlerinin farklılaşması, iç denetim birimlerinin de çağa ayak uydurmasını ve kendilerini yenilemelerini gerektirmektedir. Geçmiş yıllarda yaşanan deneyimler, paydaşların daha etkili bir güvence ve risk yönetimi beklentisini arttırmıştır. Bu yeni iş çevresinde iç denetim, ortaya çıkan değişimlere hızla cevap vermeli, daha çok risk temelli bir denetim anlayışı geliştirmeli, çalışma kağıtlarını modernize etmeli, özellikle siber suçlar gibi gündemden güne önemini arttıran alanlarda uzmanlığını arttırmalıdır.

Deloitte tarafından 2017 yılında hazırlanan “Çevik olmak: iç denetimin performans ve değerini yükseltmek için bir rehber” başlıklı çalışmada modern bir iç denetim modeli önermektedir. Buna göre çeviklik, maliyetleri ve denetim sürelerini azaltırken denetimin kalitesini arttırmak anlamına gelmektedir. Çevik bir iç denetim, paydaşların ihtiyaçlarına odaklanmayı, denetim döngüsünü hızlandırmayı, boşa harcanan emeği azaltmayı ve daha az belge yaratma anlayışını benimsemeyi kapsamaktadır.

Çevik iç denetim yaklaşımı, rutin ve standart bir iç denetim modelinden ziyade, çıktıyı temel alan, özellikli hususların belirli alanlarda uzmanlaşmış denetim personeli tarafından yerine getirildiği, tam zamanında gerçekleştirilen ve sürekli iletişimi içeren bir yaklaşımdır. Çevik bir iç denetim birimi, katı bir şekilde yıllık olarak planlanan denetimler gerçekleştirmek yerine ihtiyaç duyulduğunda veya yeni bir risk ortaya çıktığında denetimi gerçekleştirmeyi ve bu denetimleri hızla sonuçlandırmayı amaçlamalıdır. (Deloitte, 2017)

3. Bankalarda İç Sistem Olarak İç Kontrol

Henüz modern iç kontrol yaklaşımlarının ortaya çıkmadığı 1900'lü yılların başında dahi kontrol, bir yönetim fonksiyonu olarak tanımlanmıştır. Fayol kontrolü, yönetimin 5 temel unsurundan biri olarak ortaya koymuştur. Ona göre kontrol "Her şeyin verilen emirlere ve varolan kurallara uygun şekilde olmasını gözetlemektir." (Şengül, 2007). İç denetim ise bağımsızlık ve objektiflik ilkeleri gereği yönetimden ayrı olarak tasarlanmıştır. Bankaların karşılaştıkları risklere yönelik yeterli veya etkili aksiyonların alınmaması sonucunda ortaya çıkan olumsuz etkiler açısından iç denetimin, eğer önemli bir denetim hatası söz konusu değilse, bu hatalardan kaynaklanan bir sorumluluğu bulunmamaktadır. Ortaya çıkan bu olumsuz etkilerde sorumluluğun yalnızca üst yönetim ve/veya eksikliğe yer veren ilgili personel üzerinde olması, bu eksiklik ve hataların önüne geçebilmek üzere yönetim, çalışanlar ve bütün paydaşların dahil olduğu bir risk yönetimi modeli ortaya koyma ihtiyacını doğurmuştur.

Uluslararası bankacılık sektöründe geçmiş yıllarda yaşanan gelişmeler, yürütülen bağımsız iç denetim faaliyetlerinin yanı sıra, risklerin yönetilmesi için banka yönetimlerine ve bir bütün olarak işletmeye de görev ve sorumluluk yüklemeyi gerekli kılmaktadır. Bu kapsamda bankaların kendi bünyelerinde oluşturacakları iç kontrol sisteminin önemi giderek artmaktadır.

Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (COSO), beş özel sektör kuruluşundan oluşan ve 1985 yılında kurulan bir özel sektör girişimidir. COSO'nun amacı kurumsal risk yönetimi, iç kontrol ve hile caydırıcılığı üzerine çalışmaların geliştirilmesidir. Bu amaçla 1992 yılında yayınlanan ve 2013 yılında güncellenmiş olan "İç Kontrol-Bütünleşik Çerçeve" de iç kontrol, "bir işletmenin yönetim kurulu, yönetimi ve diğer personelinden etkilenen, faaliyetlerin etkililiğinin ve verimliliğinin sağlanması, güvenilir finansal raporlama ve mevcut düzenlemelere uyum konusunda makul güvence sağlamak üzere tasarlanmış bir süreç" olarak tanımlanır. COSO, kuruluşların hedeflerini operasyonel hedefler, raporlama hedefleri ve uyum hedefleri olmak üzere üçe ayırmaktadır. Bu hedefler doğrultusunda işletme geneli, bölüm, iş birimi ve şubeler özelinde kuruluşun hedeflerine ulaşmasına yardımcı olacak olan iç kontrol, beş bileşenden oluşmaktadır (COSO, 2013):

- Kontrol Ortamı: İç kontrolün kuruluş çapında uygulanmasını sağlayan standartlar, süreçler ve yapıları içerir.
- Risk değerlendirmesi: Kuruluşun hedeflerine ulaşmak için risklerin dinamik ve kendini tekrarlayan bir şekilde değerlendirilmesini içeren süreçtir.
- Kontrol faaliyetleri: Kuruluşun hedeflerine ulaşabilmesi için, politika ve prosedürler doğrultusunda risklerin yönetilebilmesi için yönetime yardımcı olan faaliyetlerdir.
- Bilgi ve iletişim: İhtiyaç duyulan bilgilerin elde edilmesi ve bunun ilgili taraflara zamanında ulaştırılmasını içerir.
- İzleme Faaliyetleri: Banka içerisinde oluşturulan politika ve prosedürler ile belirlenen kontrollerin etkinliği ve verimliliğinin sürekli olarak izlenmesi sürecidir.



Şekil 1: İç Kontrolün Bileşenleri (COSO, 2013)

İç denetim, bağımsız bir yapı olarak karşımıza çıkarken, iç kontrol tanımı gereği yönetim kurulu, yönetim ve her kademedeki çalışan tarafından etkilenen bir süreç olarak tanımlanmaktadır. Bu açıdan değerlendirildiğinde iç kontrol, kabul edilen risklerin yönetilmesi için yönetim kurulunun sorumluluğunda, üst yöneticiler tarafından kurulması gereken bir sistemdir. Risk yönetiminde bu sorumlu yaklaşım, yalnızca eksik veya hatalı

işlemlerin tespitini değil, aynı zamanda eksikliklerin ve hataların daha ortaya çıkmadan önüne geçmeyi kapsamaktadır. Sorunu kaynağında tespit etmeyi içeren önleyici ve tespit edici kontrol maliyetlerinde bir artış, toplam kalite maliyetinde azalma ve kalite düzeyinde yükselmeye sebep olmaktadır. (Kazaz & Birgönül, 2005)

Basel Komitesi, güçlü bir iç kontrol sisteminin, bağımsız bir iç denetim fonksiyonunu da içine alacak şekilde, etkili bir kurumsal yönetişimin parçası olduğunu belirtmiştir. İç denetim fonksiyonu, banka yönetim kurulu ve üst yönetimine, iç kontrol, risk yönetimi ve yönetişim sisteminin verimli çalıştığına dair güvence vererek bankanın maruz kalacağı riskleri azaltmasına yardımcı olmaktadır. (Basel Komitesi, 2015)

Basel Komitesi'nin 1998 yılında yayınladığı "Bankalarda İç Kontrol Sistemi" isimli çalışmada yönetim kurulu ve üst yönetimin görevleri açıkça tanımlanmıştır. Bu kapsamda işletme stratejilerinin ve başlıca politikalarının yönetim kurulları tarafından belirlendiğinden bahsedilmiştir. Önemli risklerin anlaşılması, bunlara ilişkin kabul seviyelerinin belirlenmesi ve üst yönetim tarafından gerekli aksiyonların alınmasının sağlanması yönetim kurulunun sorumluluğundadır. Dolayısıyla etkin bir iç kontrol sisteminin kurulması ve sürdürülmesi de yönetim kurulunun sorumluluğundadır. Üst yönetimin görevi ise, yönetim kurulu tarafından belirlenen politikalar ve risk kabul seviyeleri kapsamında süreçleri tesis etmek ve uygulamak, bu riskleri ölçmek, izlemek ve kontrol altında tutmak, görevleri ilgili personellere açık bir şekilde atamak, etkin bir iç kontrol sistemini oluşturmak ve bu sayılanlar vasıtasıyla işletmeye değer katmaktır.

Amerikan Federal Mevduat Sigorta Kurumu (FDIC) tarafından iç kontrol, karşılaşılan riskleri azaltmak ve operasyonel, raporlama ve uyum hedeflerine ulaşmak için finansal kuruluşların oluşturması gereken prosedür ve politikalar olarak tanımlanır. (FDIC, 2009) COSO'nun yapmış olduğu iç kontrol tanımıyla da uyumlu olan bu tanıma göre de iç kontrolün beş adet bileşeni olduğu belirtilmiştir. Bu bileşenleri kapsayan temel iç kontroller ise aşağıdaki tabloda özet olarak sunulmuştur.

Tablo 1: Temel İç Kontroller (FDIC, 2014)

Temel Kontroller	Kontrollerin Kapsamı
Yönetim kurulu onayı	Üst yönetimin, finansal ve operasyonel raporları düzenli olarak yönetim kuruluna sunmalıdır. Yönetim kurulu veya ilgili alt komitesi, verilen bütün önemli kararları gözden geçirmeli ve onaylamalıdır.
Uygun bir çalışan politikası	Nitelikli çalışanların işe alınması, sürekli eğitim programları ile çalışan profilinin yükseltilmesi, periyodik performans değerlendirmesi
Görevlerin ayrılığı	Bir kişinin yetkisiz olarak iş ve işlemler gerçekleştirme- sinin önüne geçmek üzere görevlerin ayrılmasıdır. Bir çalışanın yaptığı iş ve işlemi, başka bir yetkilinin onay- laması ve bu işlemin kayıt altına alınmasını içerir.
Müşterek sorumluluk	Bir varlığın veya kaydın fiziki olarak korunmasında iki veya daha fazla kişinin birlikte sorumlu olmasıdır.
İzin politikası	Çalışanların belirli bir dönem ve kesintisiz olarak yapmış oldukları görevleri bırakmasını içerir. Çalışanlara izin kullandırılması veya görev değişimi ola- rak uygulanabilir.
Çalışan rotasyonu	Personelin niteliksel gelişimini desteklemek üzere farklı pozisyonlarda deneyim kazandırılmasını içerir.
Belgelerin kayıt altına alınması	Finansal kurumların gerçekleştirdiği işlemlerde yetki- lileri belirlenmiş ve prosedürleri tanımlanmış belgeler kullanmasıdır.
Nakit kontrolü	Finansal kurumlarda görevli gişe görevlilerinin her bi- rinin ayrı bir kasadan işlem yapmasıdır. Ortak kasa kul- lanılması bireysel sorumluluğu ortadan kaldıracığı için önerilmez.
Düzensizlik ve eksikliklerin raporlanması	Ortaya çıkan eksikliklere karşı zamanında önlem alınma- sını teminen bildirim sistemi kurulmasını içerir.

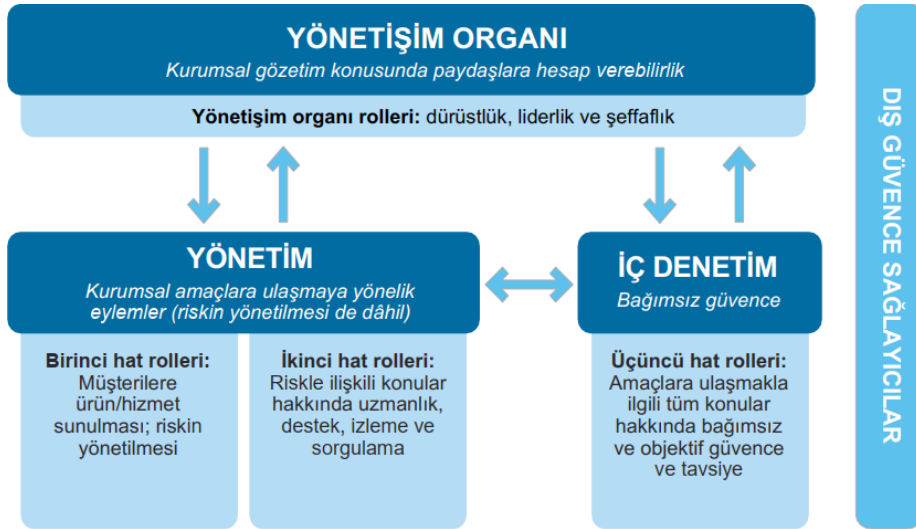
İş sürekliliği planı	Doğal afet, teknik problem veya kötü niyetli saldırıların olumsuz etkilerine karşı işlemlerin aksamaması için bir afet planını içerir. Yönetim, finansal varlıklar ve kayıtların fiziksel olarak korunması ve yaşanacak operasyonel kesintilerin minimize edilmesi için bir plan oluşturmalıdır.
Muhasebe sistemi	Doğru ve güvenilir bir bilgi ve raporlama sistemi kurulmasının içerir. Yapılan iş ve işlemler uygun olarak belgelendirilmelidir.
Denetim izi	Gerçekleştirilen iş ve işlemlerin izini sürmek üzere kayıt tutma sistemi oluşturulmasını içerir.
Muhasebe kılavuzu	Gerçekleştirilen iş ve işlemlerde karışıklık yaşanmaması için çalışanlara yardımcı olmak üzere muhasebe kılavuzu oluşturulmasını içerir.

Yukarıda yer alan iç kontroller, esasen bankaların kurması gereken iç kontrol sisteminin yalnızca bir kısmını kapsamaktadır. Değişen ve giderek daha da karmaşıklaşan iş çevresi içerisinde günümüzde özellikle bilgi teknolojileri (BT) kontrolleri önemini arttırmaktadır. BT kontrolleri, temel olarak BT genel kontrolleri ve uygulama kontrolleri olmak üzere ikiye ayrılmaktadır. BT genel kontrolleri, belirli bir kurumun bütün sistem bileşenlerini ve süreçlerini kapsayan kontrollerdir. Bunlara örnek olarak BT kontrol ortamının oluşturulması ve geliştirilmesi, BT politika ve prosedürlerinin oluşturulması, BT ile ilgili görev ayrılıklarının açıkça tanımlanması ve altyapı kontrolleri örnek olarak verilebilir. Uygulama kontrolleri ise, belirli bir iş sürecini kapsar ve girdi, işleme ve çıktı kontrollerini içerir. Bu kontroller önleyici, tespit edici ve düzeltici kontroller olarak sınıflandırılmaktadır.

Son yıllarda ortaya çıkan siber risklerin de yadsınamaz etkisi ile karmaşıklaşan iş çevresinde bankaların maruz kaldıkları risklerin kurumsal olarak yönetilmesine ilişkin yeni bir yaklaşım getiren üçlü savunma hattı modeli, risk yönetimi ve kontrol mekanizması kapsamında temel görevleri tanımlayarak, kurum içi iletişimin etkili bir şekilde artırılmasını ve bunun sonucunda risk yönetiminde etkinliğin sağlanmasına yönelik bir model önermektedir. Uluslararası İç Denetçiler Enstitüsü'ne göre organizasyonel amaçları gerçekleştirmede üst yönetimin sorumluluğu hem birinci hem de ikinci savunma hattının rollerini kapsamaktadır.

Birincil savunma hattı, daha çok mal ve hizmetlerin müşterilere teslimi ve destek hizmetleri ile ilişkilidir. Birinci savunma hattı bir üst yönetim faaliyeti olarak kurumun amaçlarına ulaşması için gerekli faaliyetleri kapsamaktadır. Buna göre yönetim kurulu ile koordineli olarak kurumun amaçlarıyla ilgili planlar yapmakta ve bu planlara ilişkin yönetim kurulu rapor vererek, iç kontrol sisteminin kurulabilmesi için uygun yapıyı oluşturmakta ve yasal zorunluluklara uyumu sağlamaktadır. İkinci savunma hattı ise risk yönetimi sürecine yalnızca tamamlayıcı bir uzmanlık desteği vermek şeklinde veya süreç içerisinde çok daha etkin rol alan bir yapı olarak karşımıza çıkabilmektedir. İkinci savunma hattı genel olarak iç kontrol de dahil olmak üzere süreçlerin uygulanması, geliştirilmesi ve iyileştirilmesini içermektedir (Uluslararası İç Denetçiler Enstitüsü, 2020).

Birinci ve ikinci savunma hatları birbirine bütünleşik tek bir fonksiyon olarak ortaya çıkabileceği gibi ikinci savunma hattı, birinci savunma hattına tamamlayıcı bir uzmanlık da sağlayabilmektedir. İkinci savunma hattı genel olarak risk yönetimi sürecinin iç kontrol, uyum ve sürdürülebilirlik gibi belirli amaçlarına hizmet etmektedir. Ancak her koşulda risk yönetimi sürecinin sorumluluğu birincil savunma hattını oluşturan üst yönetimin üzerindedir. Üçüncü savunma hattını ise bağımsız ve tarafsız bir güvence sağlayan iç denetim fonksiyonu oluşturmaktadır.



Şekil 2: Üçlü Savunma Hattı Modeli (Uluslararası İç Denetçiler Enstitüsü, 2020)

Üçlü savunma hattı yaklaşımında her üç hattın da kendine özgü rolleri vardır. Birinci savunma hattı risk yönetimi sürecinin üstlenicisidir. Bankalar açısından düşünüldüğünde şubeler ve birimler riskleri üstlenen birinci savunma hattını oluşturmaktadır. Karşılaşılan riskleri yönetmek işte bu şube ve birimlerin görevidir. İkinci savunma hattı ise risklerin tespitini, izlenmesini ve raporlanmasını içerir. İkinci savunma hattı bu görevleri yerine getirirken birinci savunma hattından bağımsız olarak çalışır. Ancak yürüttüğü faaliyetlerde amaç risk yönetimi sürecinde yönetime destek olmaktır. Dolayısıyla bir açıdan yönetim faaliyetlerinin tamamlayıcısı konumundadır. Uyum çalışmaları da ikinci savunma hattının görevleri arasındadır. İç denetim fonksiyonu ise üçüncü savunma hattı olarak hizmet vermek üzere risk bazlı genel denetimler gerçekleştirir. Bu kapsamda iç denetim fonksiyonu, iç kontrol ve risk yönetimi sistemleri de dahil olmak üzere, birinci ve ikinci savunma hattı faaliyetlerini bağımsız ve tarafsız olarak denetler ve bunların etkin olarak çalıştığına ilişkin güvence vermektedir. (Uluslararası İç Denetçiler Enstitüsü, 2013)

İçinde bulunulan ülke mevzuatına göre, büyüklükleri veya kendilerine özgü durumlar gibi farklı nedenlerle üçlü savunma hattını nasıl yapılandıracakları bankadan bankaya değişebilmektedir. Ancak nasıl yapılandırılmış olursa olsun savunma hatlarının görev ve yetkileri açıkça tanımlanmalıdır.

4. Türkiye'deki İç Sistemler Uygulamaları

Her ne kadar İngilizce'de "kontrol" ve "denetim" kelimeleri iki farklı kavrama karşılık gelse de Türkiye'de bu iki kavram sıklıkla karıştırılmakta ve birbirinin yerine kullanılabilir. Kavramların tanımını doğru yapmak, kavrama karşılık gelen şeyi doğru bir şekilde anlamamıza yardımcı olacaktır. Denetim ve kontrol konusunda Türkiye'de yaşanan karmaşanın ana sebebi, tanımların birbirini tekrar eden ve güncelliğini yitirmiş kaynaklardan alınması ve düzenleme yetkisi olan kurumların her birinin birbirinden bağımsız olarak kendi çeviri anlayışını benimsemesinden kaynaklanmaktadır. (Cömert, 2016)

5411 sayılı bankacılık kanununa göre bankalar, maruz kaldıkları riskleri yönetmek üzere, tüm şube, iş birimi ve ortaklıklarını kapsayacak şekilde yeterli ve etkin bir iç kontrol, risk yönetimi ve kurumsal yönetim sistemi kurmak zorundadır. Bu kapsamda uyum faaliyetleri, muhasebe sisteminin güvenilirliği, görevler ayrılığı, yetki ve sorumlulukların paylaşı-

mı, varlıkların korunması ve maruz kalınan her türlü riskin yönetilmesini ve yeterli iletişim ağını her seviyedeki personel tarafından uyulacak sürekli kontrol faaliyetleri ile sağlamak zorundadır. Bu kontrol faaliyetlerinin, yönetim kuruluna bağlı olarak çalışacak iç kontrol birimi ve personeli tarafından yürütülmesi öngörülmüştür. Bankacılık kanununda temel olarak sayılan bu kontrollerin, FDIC tarafından sayılan temel kontrollerle büyük ölçüde örtüştüğü görülmektedir. Ancak FDIC tarafından yayınlanan kılavuzda bağımsız bir iç kontrol birimi ve personelinden bahsedilmemiştir. Aksine COSO tanımıyla uyumlu olarak iç kontrol, firmanın yönetim ve bütün çalışanlarından etkilenen bir süreç olarak tanımlanmıştır.

Bankacılık kanununda iç kontrolün genel bir tanımı yapılmış ve bankaların iç sistemlerine ilişkin kuralların BDDK tarafından yayınlanacak bir yönetmelikle belirleneceği belirtilmiştir. Türk bankalarının karşı karşıya kaldığı riskler ve bunların ekonomiye olumsuz yansımalarının önüne geçilebilmesi amacıyla 2001 yılında Bankacılık Düzenleme ve Denetleme Kurulu (BDDK) tarafından “Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmelik” yayınlanmıştır. İlgili yönetmelikle bankaların iç kontrol merkezi adı altında bir birim kurması ve bu birimin doğrudan yönetim kuruluna bağlanmasına karar verilmiştir. Bu yönetmeliğin güncellenmiş hali olan ve 2014 yılında yayınlanan “Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik” bugün Türk bankalarındaki iç sistemler yapısının temelini oluşturmaktadır.

Buna göre iç kontrol biriminin görevleri arasında muhasebe kayıtları ve finansal raporların doğruluğu ve güvenilirliğinin kontrolü, operasyonların verimliliğini ve etkinliğini sağlamak üzere operasyonel faaliyetlerin kontrolü, varlıkların fiziki kontrolü ve mutabakatı, iletişim kanallarının ve bilgi sistemlerinin kontrolü, gerçekleştirilen iş ve işlemlerinin banka içi ve ilgili mevzuata uyumu bulunmaktadır. İlgili yönetmelik incelendiğinde, iç kontrol birimine verilen bu görevlerinin tamamının iç denetim biriminin de görevleri arasında bulunduğu görülmektedir.

Tablo 2: Türk Bankalarındaki İç Sistemler Yapısı

Banka Adı	İç Sistemler Yapısı	İç Denetimin Görevleri	İç Kontrolün Görevleri	Kaynak
Türkiye Cumhuriyeti Ziraat Bankası A.Ş	İç Sistemler Genel Müdür Yardımcılığı aracılığıyla Yönetim Kuruluna bağlı Teftiş Kurulu Başkanlığı, İç Kontrol ve Uyum Bölüm Başkanlığı ile Risk Yönetimi Bölüm Başkanlığından oluşmaktadır.	Banka'nın tüm birim ve şubeleri ile iştiraklerin faaliyetlerinin iç ve dış mevzuat doğrultusunda etkinlik ve verimlilik denetlemektedir. Denetimler, denetim programı çerçevesinde yerinden ve merkezden gerçekleştirilmektedir.	Banka'nın tüm birim ve şubeleri ile iştiraklerinin faaliyetlerinin gerek iç gerekse dış mevzuat ile uyumlu bir şekilde yürütülmesine katkı sağlamaktadır. Kontroller, kontrol programları çerçevesinde yerinden ve merkezden gerçekleştirilmektedir.	2020 Entegre Faaliyet Raporu
Türkiye Vakıflar Bankası T.A.O.	Denetim Komitesi aracılığıyla Yönetim Kuruluna bağlı Teftiş Kurulu Başkanlığı, İç Kontrol Başkanlığı, Risk Yönetimi Başkanlığı ile Uyum ve Mevzuat Başkanlığı'ndan oluşmaktadır.	Banka'nın tüm iş birimleri, şubeleri ve ortaklıklarının faaliyetlerinin iç ve dış mevzuata uygunluğunu Yerinden ve merkezden denetlemektedir. Ek olarak inceleme ve soruşturma faaliyetlerini de yerine getirmektedir. Hazırlanan yıllık denetim planı kapsamında 2020 yılında 479 şube, 12 iş birimi, 4 iştirak ve 26 bölge müdürlüğü denetimi gerçekleştirilmiştir.	Banka'nın faaliyetlerinin iç ve dış mevzuata uygun olarak yürütülmesini, finansal raporlama sisteminin güvenilirliğini, banka varlıklarının korunmasını sağlamak üzere tüm iş birimi, şube ve ortaklıklarında yerinde ve merkezden kontrol faaliyetinde bulunmaktadır. Hazırlanan yıllık kontrol planı kapsamında 2020 yılında 847 şube, 30 iş birimi ve 5 iştirak kontrolü gerçekleştirilmiştir.	

Türkiye Halk Bankası A.Ş.	İç Sistemler Grup Başkanlığı aracılığıyla Yönetim Kuruluna bağlı İç Kontrol Daire Başkanlığı, Risk Yönetimi Daire Başkanlığı ve Uyum Daire Başkanlığı'ndan oluşmaktadır. Teftiş Kurulu Başkanlığı ise doğrudan Yönetim Kurulu'na bağlıdır.	Tüm şube, birim ve ortakları kapsayacak şekilde bankacılık faaliyetlerinin iç ve dış mevzuat doğrultusunda yürütülmesini ve kaynakların etkin ve verimli şekilde kullanılmasını amaçlamaktadır. Yıllık denetim planı çerçevesinde yerinde denetim, merkezden denetim ve bilgi teknolojileri denetimi gerçekleştirilmektedir. Ek olarak inceleme ve soruşturma çalışmaları yürütülmektedir.	Banka'nın varlıklarının korunması, faaliyetlerinin etkin ve verimli bir şekilde iç ve dış mevzuata uygun olarak yürütülmesi, finansal raporlama sisteminin güvenilirliğinin sağlanmasına yönelik olarak yıllık kontrol planı kapsamında tüm şube, iş birimi ve ortaklıklarda faaliyetlerini yürütmektedir. Ek olarak özellik arz eden konularda inceleme faaliyetleri yerine getirmektedir.	2020 Faaliyet Raporu
Akbank T.A.Ş.	Doğrudan Yönetim Kurulu'na bağlı İç Kontrol Başkanlığı, Teftiş Kurulu Başkanlığı, Risk Yönetimi Başkanlığı, Uyum Başkanlığı ve Bilgi Riski Yönetimi Başkanlığı'ndan oluşmaktadır.	Banka'nın tüm şube, iş birimi ve ortaklıklarının faaliyetlerinden kaynaklanabilecek risklerin yönetilmesi, gerçekleştirilen işlemlerin iç ve dış mevzuata uyumu, verimlilik ve performansın geliştirilmesi ve varlıkların korunmasına yönelik denetim faaliyetleri gerçekleştirilmektedir.	Banka'nın faaliyetlerinin etkin ve verimli bir şekilde iç ve dış mevzuata uygun yürütülmesini sağlamak amacıyla tüm şube ve iş birimlerinde gerek yerinden gerekse merkezi olarak kontrol çalışmaları yürütmektedir.	2020 Faaliyet Raporu

Yapı ve Kredi Bankası A.Ş.	Denetim Komitesi aracılığıyla Yönetim Kurulu'na bağlı Uyum, İç Kontrol ve Risk Yönetimi Genel Müdür Yardımcılığı ve İç Denetim Yönetimi Genel Müdür Yardımcılığından oluşmaktadır.	Olağan şube denetimi, süreç denetimi, soruşturma ve takip denetimini kapsamaktadır. Yönetim prosedürlerinin ve iş süreçlerinin etkinliği ve yeterliliği risk açısından değerlendirilir. Yıllık denetim planı kapsamında 2020 yılında toplam 342 şube, 56 ortaklık ve 40 iş biriminde denetim çalışmaları yürütülmüştür. İç Denetim Yönetimi bünyesinde 149 çalışan görev yapmaktadır.	Banka'nın şube ve iş birimlerinde iç ve dış mevzuat kapsamında belirli aralıklarla kontrol faaliyeti gerçekleştirmektedir. Yıllık kontrol planı kapsamında 300 şube ve 8 ortaklıkta yerinde denetimler gerçekleştirilmiştir. İç kontrol faaliyetleri kapsamında toplam 102 çalışan görev yapmaktadır. Gelecek dönemlerde dijital dönüşüm süreci çerçevesinde merkezden kontrol çalışmalarının artırılması hedeflenmektedir.	2020 Entegre Faaliyet Raporu
Türkiye İş Bankası A.Ş.	Doğrudan Yönetim Kurulu'na bağlı Teftiş Kurulu Başkanlığı, Risk Yönetimi Bölümü, Kurumsal Uyum Bölümü ile İç Kontrol Bölümü'nden oluşmaktadır.	Bankanın tüm şube, iş birimi, süreç ve bilgi sistemlerinin faaliyetlerinin iç ve dış mevzuat doğrultusunda denetimini gerçekleştirmektedir. Gerektirdiği takdirde ön araştırma, inceleme ve soruşturma faaliyetleri de yürütmektedir.	Süreç sahiplerince yürütülen iç kontrol faaliyetlerinin tasarım ve işletim etkinliği, bağımsız bir fonksiyon olan İç Kontrol Bölümünce de düzenli olarak incelenmektedir. Bu kapsamda yıllık kontrol planı dahilinde tüm şube, iş birimi ve ortaklıkların iç kontrol yapılarına yönelik yerinde ve merkezden incelemeler yürütülmektedir.	2020 Faaliyet Raporu

Türk bankalarında ortaya çıkan bu iç kontrol yapısı, özellikle kamu bankalarında, hazırlanan yıllık kontrol planı kapsamında şube, iş birimi ve ortaklıkların fiziki kontrolünü ve iç kontrol merkezinden yapılan bilgi teknolojileri kontrollerini içermektedir. Hatta bazı Türk bankalarında iç kontrol biriminde görev yapan personelin, teftiş kurullarında görülen soruşturma yetkisine benzer bir inceleme yetkisi verildiği de uygulamada karşımıza çıkmaktadır. İç kontrol personeli, yaptığı bu kontrol ve incelemeler sonucunda tespitlerini bir rapora bağlar ve bunu ilgili birimlere tebliğ eder. Bu kapsamda, Türk bankacılığında iç kontrol ve iç denetim birimlerinin yetki ve sorumlulukları, ilgili kanun ve yönetmeliklerde de açıkça görülebileceği gibi iç içe geçmiştir.

Temel olarak aynı işi yapan ve hemen hemen benzer yetki ve sorumlulukları bulunan iç kontrol ve iç denetim birimleri, görev yaptıkları konular itibarıyla da benzeşmektedir. Öyle ki yıllık denetim ve kontrol planları kapsamında aynı şubeler ve birimler, hem iç kontrol hem de iç denetim birimi tarafından ayrı ayrı denetlenmekte ve kontrol edilmektedir. Bu da yapılan denetim ve kontrollerin tekrarına ve gösterilen çabaların mükerrer olmasına sebep olmaktadır. Ortaya çıkan bu mükerrer denetim, bankaların maliyetlerini artırmakta ve kaynak kullanımında verimsizliğe sebep olmaktadır.

5. Öneriler ve Değerlendirmeler

2008 yılında yaşanan küresel ekonomik kriz, yönetim sistemleri oturmuş bankaların bile finansal zorluklar yaşayabileceğini ve hatta batabileceğini dünya kamuoyuna göstermiştir. Bu küresel ekonomik kriz özellikle bağımsız denetim ve iç denetim faaliyetlerinin geleceğini geri dönülemez bir biçimde değiştirmiştir. Türk bankacılık sektöründe oturmuş bir sistem olan teftiş kurullarının da değişimlerden etkilenmesi kaçınılmazdır. Geleneksel iç denetim yaklaşımının yerini sorumlu bir risk yönetimi anlayışına bırakmaya başladığı ve yeni iç sistemler yaklaşımının her geçen gün önemini arttırdığı görülmektedir.

Diğer yandan Dünya çapında yaşanan teknolojik gelişmeler, geleneksel bankacılığın yerini şubesiz bankacılık kanallarına bırakmasına sebep olmaktadır. Müşteri ile çalışan arasında etkileşimi minimuma indiren bu yeni teknolojiler, müşterilerin banka şubelerine gitmeksizin işlemlerini yapmasına sebep olmakta ve geçmişte çalışanlar eliyle yapılan birçok müşteri işleminin, kurulan sistemler aracılığıyla ve çalışan müdahalesine gerek duymak-

sızın yapılmasını sağlamaktadır. Bu da geleneksel denetim birimlerinin gerçekleştirdiği yerinde denetimlerin çerçevesinin giderek daralmasına sebep olmaktadır. İç denetim birimleri vasıtasıyla yürütülen düzeltici denetimler, yerini önleyici ve tespit edici kontrollere bırakmaktadır. Süreçleri tasarlarken oluşturulacak dijital kontrol mekanizmalarının, insan kaynaklı hataları azaltacağı ve toplam kaliteyi yükselteceği öngörülmektedir. Dijital kontrol mekanizmalarının eksiklik veya hatayı daha gerçekleşmeden tespit etmesi sayesinde düzeltici denetim maliyetlerinde de bir azalış olacağı tahmin edilmektedir. Dijital kontrol mekanizmalarının yaygınlaştırılmasının bir diğer yadsınamaz katkısı ise oluşturulan kontrollerin daha geniş bir örneklemi kapsamasıdır. Günümüzde büyük verinin denetiminde daha geniş bir örneklem, hatta gerçekleştirilen bütün iş ve işlemlerin kontrolü söz konusu olabilmektedir. Daha geniş bir evrende gerçekleştirilen kontroller sayesinde hata olasılığının da büyük oranda azalacağı tahmin edilmektedir.

Bankaların entegre faaliyet raporları incelendiğinde iç kontrol biriminin, bankanın faaliyetlerinin iç ve dış mevzuata uygun olarak yürütülmesine yardımcı olmakla görevli olduğu görülmektedir. Ancak Türk bankacılık uygulamasında iç kontrol birimleri, öz değerlendirme de dahil olmak üzere, yönetimin politika ve prosedür oluşturma sürecine dahil olmamaktadır. İç kontrol, politika ve prosedürlerin oluşturulması sürecinin içerisinde yer almak yerine, bir denetim fonksiyonu gibi hareket ederek politika ve prosedürlerin iç ve dış mevzuata uygunluğunu denetlemekte ve tespit edilen eksiklikleri yönetim kurulu ve üst yönetime raporlayan bir denetim gerçekleştirmektedir. Türkiye’de oluşan ikili denetim mekanizmasının önüne geçmenin bir yolu da iç kontrol mekanizmasının, uluslararası örnekler doğrultusunda politika ve prosedürlerin oluşturulması sürecine dahil edilmesidir. İç denetimin görevi ise politika ve prosedürlerin iç ve dış mevzuat doğrultusunda etkinlik ve verimliliğini denetlemek olmalıdır. Bu yaklaşım COSO ve Uluslararası İç Denetçiler Enstitüsünün önerdiği “Üçlü Savunma Hattı” modeli ile de uyumlu bir yaklaşım olacaktır.

Emek yoğun denetimlerin önemini yitirmesi ve çevik bir denetim anlayışı ile yalnızca ihtiyaç duyulduğunda gerçekleştirilecek hızlı ve kısa süreli yerinde denetimler sayesinde bankaların iç denetim birimleri daha az sayıda çalışan ile daha uzmanlaşmış bir alanda hizmet verebilecektir. Şekil değiştiren risklerle başa çıkmak üzere, ihtiyaç duyulduğunda denetimleri gerçekleştirecek çevik bir iç denetim birimi ve bunu desteklemek üzere, yö-

netim tarafından kurulan yaygın bir iç kontrol sistemi hem risk yönetimi maliyetlerini düşürecek, hem de aynı işin mükerrer olarak yapılmasını engelleyecektir.

Çevik iç denetim yaklaşımı, etkin ve yaygın bir iç kontrol yapısını gerekli kılmaktadır. Buna göre insan etkisinin her gün azaldığı bir bankacılık çevresinde rutin iç denetimlerin gerçekleştirilmesi, gereksiz efor sarfetmek anlamına gelecektir. Yıllık olarak yapılan katı iç denetim planları, risk içermeyenler de dahil bir çok işlemin denetlenmesini gerektirmektedir. Bu ihtiyacı karşılamak üzere bankalar geniş bir iç denetim birimi oluşturmak ve çok sayıda iç denetim personeli istihdam etmek zorunda kalmaktadır.

Türk Bankacılık sisteminde halihazırda uygulanan iç kontrol ve iç denetim yapısını, iki başlı denetim olarak değerlendirmek ve bu şekilde uygulamak yerine, iç kontrol faaliyetlerini geleneksel teftiş kültüründen modern iç denetime geçiş için bir fırsat olarak değerlendirmek önemlidir.

Uygulanacak bu yeni iç sistemler yaklaşımının, hem maruz kalınan riskleri yönetmede daha etkili olacağı, hem de denetim maliyetlerini önemli ölçüde düşüreceği düşünülmektedir. Buna ek olarak bu yaklaşım, Türk bankalarındaki iç sistemler yapısının uluslararası standartlara ve uygulamalara uyumunu da sağlayacaktır.

Yazar Katkısı

Çalışmada literatür taraması ve sonuçların değerlendirilmesi Yağızcan Yücel Çendik tarafından yapılmıştır. Doç. Dr. Duygu Anıl Keskin bu çalışmanın tüm aşamalarında görüş ve fikirleri ile katkı sunmuştur.

Çıkar Çatışması

Yazarlar arasında bir çıkar çatışması bulunmamaktadır.

Finansal Destek

Yazarlar bu çalışma için herhangi bir finansal destek almamıştır.

Hakem Değerlendirmesi

Dış Bağımsız

Kaynakça

5411 sayılı bankacılık kanunu (2005). T. C. Resmi Gazete, 25983, 01 Kasım 2005.

Akbank T.A.Ş. (2021). 2020 Akbank faaliyet raporu. Erişim adresi: https://www.akbankinvestorrelations.com/tr/images/pdf/faaliyet-raporlari/2020_akbank_faaliyet_raporu_.pdf.

Bankaların iç sistemleri ve içsel sermaye yeterliliği değerlendirme süreci hakkında yönetmelik (2014). T.C. Resmi Gazete, 29057, 11 Temmuz 2014.

Basel Committee on Banking Supervision. (1998). Framework for internal control systems in banking organizations. Retrieved from: <https://www.bis.org/publ/bcbs40.pdf>.

Basel Committee on Banking Supervision. (2002). Internal audit in banks and the supervisor's relationship with auditors: A survey. <https://www.bis.org/publ/bcbs92.pdf>.

Basel Committee on Banking Supervision. (2012). The internal audit function in banks. Retrieved from: <https://www.bis.org/publ/bcbs223.pdf>.

Basel Committee on Banking Supervision. (2015). Guidelines: Corporate governance principles for banks. Retrieved from: <https://www.bis.org/bcbs/publ/d328.pdf>.

Committee of Sponsoring Organizations of The Treadway Commission. (2013). Internal control-integrated framework.

Cömert, N. (2016). İşletmelerde kontrol ve denetim kavramlarının doğru kullanılması amacıyla yönelik kavramsal bir inceleme. Marmara Üniversitesi Marmara Business Review, Cilt 1 (1), 1-20.

Deloitte. (2017). Becoming agile: A guide to elevating internal audit's performance and value. Retrieved from: <https://www2.deloitte.com/us/en/pages/advisory/articles/agile-internal-audit-planning-performance-value.html>.

European Monetary Institute. (1997). Internal control systems of credit institutions. Retrieved from: https://www.ecb.europa.eu/ecb/access_to_documents/document/emi_pubaccess/shared/data/ecb.dr.paremi2007_06_report.en.pdf.

Federal Deposit Insurance Corporation Improvement Act of 1991, 12 U.S.C. § 1811 et seq. (1991).

Federal Deposit Insurance Corporation. (2014). Risk management manual of examination policies. Retrieved from: <https://www.fdic.gov/regulations/safety/manual/>.

Kaufmann, G.G., & Scott, K.E. (2003). What is systemic risk, and

do bank regulators retard or contribute to it? *The Independent Review*, 8(3), 371-391.

Kazaz, A., & Birgönül, T., (2005). The evidence of poor quality in high rise and medium rise housing units: A case study of mass housing projects in Turkey. *Building and Environment*, 40, 1548-1556.

Peek, J., & Rosengren, E., S. (2000). Collateral damage: Effects of the Japanese bank crisis on real activity in the United States. *The American Economic Review*, 90(1), 30-45.

Şengül, R. (2007). Henri Fayol'un yönetim düşüncesi üzerine notlar. *Celal Bayar Üniversitesi İİBF Dergisi*, Cilt. 14 (2), 250-273.

The Institute of Internal Auditors. (2013). The three lines of defense in effective risk management. Retrieved from: <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf>.

The Institute of Internal Auditors. (2017). International professional practices framework. Retrieved from: <https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf>.

The Institute of Internal Auditors. (2020). Global technology audit guide: IT essentials for internal auditors. Retrieved from: <https://iaa.no/wp-content/uploads/2020/06/2020-GTAG-IT-Essentials-for-Internal-Auditors.pdf>.

The Institute of Internal Auditors. (2020). The IIA's three lines model: An update of the three lines of defense. Retrieved from: <https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf>.

The Institute of Internal Auditors. (2020). Küresel Bakış Açılımları ve Anlayışları: Üçlü hat modeli her kurumun başarısı için önemli bir araç. Erişim adresi: <https://global.theiia.org/translations/PublicDocuments/GPI-Three-Lines-Model-TURKISH.pdf>.

Türkiye Cumhuriyeti Ziraat Bankası A.Ş. (2021). 2020 Entegre faaliyet raporu. Erişim adresi: https://www.ziraatbank.com.tr/tr/yatirimci-iliskileri-ZB/finansal-bilgiler/Documents/2020_entegre_faaliyet_raporu.pdf.

Türkiye Garanti Bankası A.Ş. (2021). 2020 Entegre faaliyet raporu. Erişim adresi: <https://www.garantibbvainvestorrelations.com/tr/images/entegre-faaliyet-raporu-2020/pdf/garanti-bbva-2020-entegre-faaliyet-raporu.pdf>.

Türkiye Halk Bankası A.Ş. (2021). Halkbank 2020 faaliyet raporu. Erişim adresi: <https://www.halkbank.com.tr/content/dam/halkbank/tr/dokumanlar/yatirimci-iliskileri/finansal-bilgiler/finansal-bilgiler/faaliyet-raporlar%C4%B1/2020FaaliyetRaporu.pdf>.

Türkiye İç Denetim Enstitüsü. (n.d). İç denetimin tanımı. <https://www.tide.org.tr/page/26/Ic-Denetimin-Tanimi>.

Türkiye İş Bankası A.Ş. (2021). Türkiye'nin bankası 2020 faaliyet raporu. Erişim adresi: <https://www.isbank.com.tr/contentmanagement/IsbankFinancialDocuments/Y%C4%B1ll%C4%B1k%20ve%20Ara%20D%C3%B6nem%20Faaliyet%20Raporlar%C4%B1/pdf/faaliyet2020.pdf>.

Türkiye Vakıflar Bankası T.A.O. (2021). 2020 Entegre faaliyet raporu. Erişim adresi: https://www.vakifbank.com.tr/documents/yiliski/VKF_FRAT_2020_UYG__uyg_65_SPREADS_NY.pdf.

Yapı ve Kredi Bankası A.Ş. (2021). 2020 Entegre faaliyet raporu. Erişim adresi: https://www.yapikrediinvestorrelations.com/tr/images/pdf/faaliyet-raporlari/2020/yapi_kredi_2020_entegre_faaliyet_raporu.pdf?v4.

Yurtsever, G. (2009). Teftiştten iç denetime banka müfettişliği, 2009, Türkiye Bankalar Birliği

Özgeçmiş

Yağızcan Yücel Çendik, Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakültesi Kamu Yönetimi Bölümü'nden mezun oldu. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü'nde Finansal Ekonomi Bölümü'nde yüksek lisansını tamamladı. İstanbul Üniversitesi İşletme (İktisat) Anabilim Dalı'nda doktora yapmaktadır. CIA mesleki sertifikasına sahiptir. Bir bankada iç kontrolör olarak çalışmaktadır.

Doç. Dr. Duygu Anıl Keskin, İstanbul Üniversitesi İktisat Fakültesi İşletme Bölümü Muhasebe Anabilim Dalı'nda doçent olarak görev yapmaktadır. Doktora derecesini Marmara Üniversitesi Sosyal Bilimler Enstitüsü Muhasebe Finansman programında almıştır. Araştırma alanlar; bağımsız denetim, iç denetim, muhasebe kültürü, maliyet muhasebesi ve yönetim muhasebesidir.

Teorik Makale / Theoretical Article

MUHASEBE VE DENETİMDE MESLEKİ YARGININ EPİSTEMOLOJİK BOYUTU: ÖZNE-NESNE İLİŞKİSİ

Selahattin KARABINAR¹

Submitted/Başvuru: 30.05.2021

Last Revised/Son Düzeltme: 11.07.2021

Accepted/Kabul: 13.07.2021

Öz

Bilme eyleminde özne (bilen) ve nesnenin (bilinen) etkilerinin sorgulanması bilgi felsefesinin (epistemoloji) temel sorgulama alanlarından biridir. Kant'a kadar nesnenin belirleyici olduğu türden bilme eylemi kabul edilirken Kant'tan sonra öznenin de belirleyici olduğu düalist görüş hakim olmuştur. Muhasebe ve denetimde kullanılan mesleki yargıda bulunma sürecinde nesnenin baskın olduğu görüşü benimsenirse bir süre sonra (piyasa dinamizminin ortaya çıkardığı yeni durumlar hariç) tekdüze ve her şeyin oturmuş olduğu bir ortam öngörülebilir. Mesleki yargıda öznenin hakim olduğu görüşün benimsenmesi durumunda da benzer olay ve olgular hakkında birbirinden çok farklı yargılara ulaşılabileceği, bu durumun da özgün uygulamaların ortaya çıkmasına katkı sağlayacağı beklenebilir.

Anahtar Kelimeler: Bilgi Felsefesi, Bağımsız Denetim, İç Denetim, Mesleki Yargı

JEL Sınıflandırması: M14, M42, G40, M51, Z10

¹ Prof. Dr., İstanbul Üniversitesi İktisat Fakültesi İşletme Bölümü, selahattin.karabinar@istanbul.edu.tr ORCID: 0000.0003.3102.979X

To cite this article: Karabınar, S. (2021). Muhasebe ve Denetimde Mesleki Yargının Epistemolojik Boyutu: Özne-Nesne İlişkisi. *TİDE Academia Research*, 3(1), 41-54

EPISTEMOLOGICAL DIMENSIONS OF PROFESSIONAL JUDGMENT IN ACCOUNTING AND AUDITING: SUBJECT-OBJECT RELATIONSHIP

Abstract

Questioning the effects of the subject and the object in the act of knowing is one of the main fields of inquiry in epistemology. Until Kant, the act of knowing, in which the object is determinant, was accepted, but after Kant, the dualist view in which the subject was also determinant was dominant. If the opinion that the object is dominant in the process of making professional judgments used in accounting and auditing is accepted, after a while (except for the new situations brought about by the market dynamism), a uniform and settled economic environment can be estimated. In case of accepting the view that the subject is dominant in professional judgment, it can be expected that very different judgments can be reached about similar events and phenomena, and this situation will contribute to the emergence of original practices.

Keywords: Epistemology, Auditing, Internal Audit, Professional Judgement

JEL Classification: M14, M42, G40, M51, Z10

Extended Summary

Introduction

People make various evaluations and make inferences in the face of events and phenomena they encounter in daily life. The process of making evaluations and making inferences can be expressed as “the act of knowing” in general. The nature and content of the act of knowing is the subject of epistemology in philosophy. In this process, sometimes the characteristics of the observer (“subject” in the expression of epistemology) are decisive, and sometimes the result of the observed event (in the expression of epistemology “object”) is decisive.

In accounting and auditing practices, members of the profession should make an assessment and decide on the situations they encounter. This act of evaluation and decision making is an act of knowing in terms of epistemology.

In this study, the evaluation and decision process of the member of the profession is discussed in terms of epistemology (especially in terms of subject-object relationship). It is aimed to understand the nature and philosophical dimension of the professional judgment process. In the process, it has been tried to make predictions about the consequences that may arise in case of which of the subject and object is dominant.

Methodology

In this study, a conceptual method was used to explain the philosophical dimension of professional judgment through the subject-object relationship. The possible effects and results of the views put forward about the subject-object relationship in epistemology have been tried to adapt to professional judgment in accounting and auditing. In this respect, it is a conceptual study.

Conclusion

When the object is dominant in professional judgment, it can be predicted that accounting practices will evolve towards uniformity. Uniformity can be considered as a desirable result for the members of the profession, therefore it will create an environment that does

not contribute to the emergence of creativity and original practices. In environments where care is dominant, it can be expected to encounter a wide variety of judgments about the same event and phenomenon.

1. Giriş

İnsanlar günlük hayatta karşılaştıkları olay ve olgular karşısında çeşitli değerlendirmelerde bulunurlar, çıkarımlar yaparlar. Değerlendirmelerde bulunma ve çıkarım yapma süreci en genel olarak “bilme eylemi” olarak ifade edilebilir. Bilme eyleminin doğası ve içeriği felsefede bilgi felsefesinin (epistemoloji) konusudur. Bu süreçte bazen gözlem yapanın (bilgi felsefesi ifadesiyle “özne”) özellikleri belirleyici olur, bazen de gözlenen olay (bilgi felsefesi ifadesiyle “nesne”) sonucu tayin edici olur.

Muhasebe ve denetim uygulamalarında meslek mensuplarının karşılaştıkları durumlarla ilgili bir değerlendirme yapması ve karar vermesi gerekir. Bu değerlendirme ve karar verme eylemi epistemolojik açıdan bilme eylemidir.

Bu çalışmada meslek mensubunun değerlendirme ve karar süreci bilgi felsefesi açısından (özellikle özne-nesne ilişkisi açısından) ele alınmıştır. Mesleki yargıda bulunma sürecinin doğasının ve felsefi boyutunun anlaşılması amaçlanmıştır. Süreçte özne ve nesneden hangisinin baskın olması durumunda ortaya çıkabilecek sonuçlara ilişkin öngörülerde bulunmaya çalışılmıştır.

2. Epistemoloji ve Epistemolojide Özne-Nesne İlişkisi

Bu başlık altında epistemolojinin felsefedeki yeri ve çalışmanın amacına paralel olarak özne-nesne ilişkisi ele alınmıştır. Çünkü bu ilişki epistemolojinin (bilgi felsefesinin) temel sorgulama alanıdır.

2.1. Epistemoloji

Felsefenin insanın bilme eylemini konu edinen dalına epistemoloji (veya bilgi felsefesi) denilir. Sıklıkla karıştırıldığı üzere epistemolojinin (bilgi felsefesi) bilim felsefesi anlamına gelmediğine dikkat etmek gerekir. Bilgi felsefesi insanın (her türlü) bilme eylemini anlamayı ve onun doğasını açıklamayı konu edinirken bilim felsefesi bilimi ve bilimsel düşüncüyü, onun yöntem ve içeriğinin (muhtevası) ne olduğu ile ilgilenen bir felsefe alanıdır. Kısaca bilim felsefesi bilimi anlamaktır (Yıldırım, 2012). Öte yandan bu karıştırmanın bir yere kadar mazur görülebilecek nedeni vardır (Simard’dan çeviren Adıbelli, 2003). O da epistemolojik ve ontolojik sorgulamalardan bağımsız bir bilim felsefesinin mümkün olmayacağıdır. Çünkü bilimin amacı doğru bilgiye ulaşmaktır. Tam da bu noktada epistemoloji ile bilim felsefesi arasında yakın ilişki kurulmuş olur.

Bu bağlamda doğru bilginin; *a)olanaklılığı (imkanı), b)koşulları, c)kaynakları ve d)sınırlarının* ne olduğu epistemolojinin temel sorgulama noktaları olarak karşımıza çıkar (Öner, 2015). Ancak epistemolojide en önemli soru “bilme eylemi nasıl gerçekleşir” sorusudur. Bilme eyleminin odak noktasında *bilen* (özne) ile *bilinen* (nesne) vardır. Kısaca bilme *bilen* ile *bilinen* arasındaki (özne ile nesne arasındaki) ilişki olarak ifade edilir. Bu ikisi arasındaki ilişki ve etkileşim bilgi felsefesinde farklı görüşlerin ortaya çıkmasına neden olmuştur.

2.2. Özne-Nesne İlişkisi Üzerine Felsefi Görüşler

Epistemolojik açıdan bilgi edinme süreci öznenin nesneye vakıf olması, onu anlamasını ifade eden bir süreç olarak tanımlanabilir. Bu süreçte özne her zaman bir insandır ve nesne hakkında hisseden, düşünen taraf olmaktadır. Nesne de öznenin hissetmesinin ve düşüncesinin içeriğini veren şey veya durum olarak karşımıza çıkar. Felsefe tarihine bakıldığında pek çok filozofun bilme olgusu üzerine kafa yorduğu, sorgulamalar yaptığı, konu hakkında pek çok soruya cevap aramaya çalıştığı görülür². Bu çalışmanın konusu bilgi felsefesi hakkında detaylı bilgi vermek olmadığı için ayrıntıya girmek uygun görülmemiştir³. Bilme eyleminde ve dolayısıyla özne nesne ilişkisinde temel olarak aşağıdaki sorulara cevap aranmıştır (Öner, 2015). Bunlar;

- Bilme eyleminde belirleyici olan özne midir yoksa nesne midir?
- Biri diğerine baskın çıkarsa bilme eylemi nasıl şekillenir?
- Bilme eyleminde özne ve nesne dışında dışsal faktörler var mıdır? Varsa etkisi nedir?

Öznenin kişisel özellikleri nesneyi anlamlandırma şeklini belirler. Bu da duylara bağlıdır, öznel, kişiye özgüdür ve rasyonalisttir. Kant’a göre bilme eyleminde zaman ve mekan yönlendirici olmaktadır. Başka bir ifadeyle daha çok öznenin nesneyi kendi kurallarına göre belirlediği bir ilişkidir. Buna göre bilgi, zaman ve mekanın yönlendirmesi ve öznenin bu yönlendirmeleri anlama yetisi sonucu ortaya çıkmaktadır. Bu durum kısaca öznenin nesneye baskın gelmesi olarak ifade edilir ve ulaşılan bilgi “öznel bilgi” olarak adlandırılır.

Nesnenin özneye baskın çıkması durumu ise özneyi edilgen kılar. Nesne, yönlendirici olur.

2 Platon, Rene Decartes, David Hume, John Locke ve Immanuel Kant bu filozofların önde gelenleridir.

3 Detaylı bilgi için Öner, N., (2015). Bilginin Serüveni, Divan Kitabevi, İstanbul kaynağına başvurulması önerilir.

Nesnenin özellikleri özneyi değiştirir, şekillendirir. Böylesi bir ilişkide ampirik yöntem temel bir yöntem haline gelir. Nesne, ihtiyaç veya algı tarafından seçilerek öncelikle zihnimizde bir yer bulur. Sonrasında davranış edimlerimizin yöneldiği bu nesne ve bize kattığı değerler, artık dışımızda hiç bilmediğimiz değil bizzat deneyimleyip kendi yaşam sınırlarımıza kattığımız bir parçamıza -özne parçasına- dönüşür.

Bilme eyleminde Kant'a kadar Platon'cu düşünme hakimdir. Başka deyişle bilme eyleminde özneyi esas alınır. Bu düşünce tarzı rasyonalisttir, dogmatiktir, nesne yoktur. Özneye etki eden dış etkenlerin bilme eylemine etkisinin olmadığı, "*mutlak bilme*" vardır. Bu hakim düşünceye aykırı ilk görüşler David Hume'dan gelmiştir: Hume ve taraftarları ise öznenin nesneden etkilendiği noktasından hareket ederler. Bu yönüyle ampirist oldukları söylenebilir.

Kant ise nesnenin öznenin etkilendiği olgusundan hareket ederek özne-nesne arasında çift taraflı etkileşim (düalizm) öngörür. Öznenin nesneyle ilgili düşünce ve deneyimleri nesneye şekil kazandırır. Bu görüşte nesne edilgendir, düzenleme gücü yoktur. Nesnenin düzenleme gücü olmayacağına göre belirleyici ve düzenleyici olan özne olmalıdır (Göçmen 2008).

Kant'a kadar epistemolojide geçerli yaygın kabul gören görüş nesne temellidir. Kant ise bunun tam tersini iddia ederek o zamana kadar yaygın olan görüşe karşı çıkmıştır. Bu durum bilgi felsefesi tarihinde "Epistemolojide Kopernik Devrimi" olarak adlandırılır⁴. Kant'ın aşağıdaki örneği özne temelli bilme eylemine açıklık kazandırmaktadır. İçi para dolu bir kundakta yatan bebek paranın değerinden habersiz uyur. Burada eğer nesne temelli bilme eylemi olsaydı bebek içinde uyuduğu kundağın değerini bilebiliyor olurdu. Fakat bilme eylemi öznenin nesneye atfettiği anlam ile bir bütünlük kazandığı için bebek duyuları gelişip ortamı ve parayı anlamaya başlayana kadar sahip olduğu servetin farkında olmayacaktır.

3. Mesleki Yargı, Muhasebe ve Denetimde Kullanımı

Mesleki yargının (bunun yerine "mesleki muhakeme" ifadesi de kullanılmaktadır) muhasebe ve denetimde yaygın bir kullanımı vardır. Muhasebe ve denetim alanında çalışan

⁴ Kopernik'e kadar dünya (yer) merkezli (geosentrik uzay) bir evren görüşü hakim iken Kopernik güneş merkezli (heliosentrik uzay) bir evren iddiasını ortaya atmakla o güne kadar hakim olan görüşü çürütmüştür. Bu durum "Kopernik Devrimi" olarak adlandırılır.

meslek mensupları ve akademisyenlerin çok yakından bildiği üzere meslek mensubu pek çok noktada olgu ve olay hakkındaki kendi öznel değerlendirmesini kararlarına yansıtır. Bu durum aynı zamanda karar veren hemen herkes için geçerlidir.

Mesleki yargı (muhakeme): Denetimin yürütülmesi sırasında mevcut olan şartlara uygun olarak atılacak adımlara yönelik bilgiye dayalı kararlar alınırken; mevzuat, BDS'ler, muhasebe standartları ve etik standartlar çerçevesinde, sahip olunan eğitim, bilgi ve deneyimin kullanılmasıdır (BDS 200, p.13f).

Muhasebe ve finansal raporlama alanında mesleki yargı M.Gibbins ve A.Mason tarafından (Solaş,2006); finansal değerlendirme, kaydetme ve raporlama esnasında bir karara ulaşma süreci olarak tanımlanmaktadır. Denetim ve muhasebe standartlarına ve meslek ahlak yasasında belirtilen açıklamalara bağlı olarak, ilgili konudaki bilgi ve tecrübeye dayanılarak verilen karar biçiminde tanımlanmaktadır.

Mesleki yargı, ilgili mesleğin standart ve kuralları çerçevesinde, gerekli özen, tarafsızlık, bağımsızlık, dürüstlük gibi mesleki etik ilke ve kurallara bağlı kalarak, deneyimli ve bilgili meslek mensubu tarafından varılan hükümdür (Sürmen ve Bayraktar, 2015)

Mesleki yargı tanımından hareketle söz konusu yargının taşıması gereken birtakım özellikler vardır. Bunlar (Gibbins ve Mason, 1988'ten aktaran Sürmen ve Bayraktar, 2015):

- Anlamlı bir tercih içermesi,
- Sorunu tanımlama ve sorunun farkında olmadan karar vermeye uzanan bir süreci içermesi,
- Kişinin iş sorumlulukları ile ilgili olması ve kişisel düzeyde dürüstlük gibi değerleri barındırması,
- Gerekli ve disipline özel teorik ve pratik bilgiyi gerektirirken mesleki standartlar ve mevcut uygulama ile ilgili olması,
- Benzer sorunlar ve benzer durumlarla ilgili deneyime dayalı olması,
- Mesleki tarafsızlığa izin veren koşullar altında gerçekleştirilmesidir.

Uluslararası Finansal Raporlama Standartlarında mesleki yargı yaygın kullanıma sahiptir. Mesleki yargı sayesinde raporlama yapan işletmeye özgü durumların finansal raporlara yansıtılması sağlanmış olur. Standartlar uygulayıcıların bireysel yargıları olmaksızın

düzgün şekilde çalışamazlar (Dalkılıç,2008). Diğer bir ifadeyle mesleki yargının sağladığı esneklik ve kavrama olmadan finansal muhasebe prosedürleri, standartları ve kuralları hantal, sonuçsuz ve işlevsiz hale gelebilir.

Mesleki yargının farklı türleri vardır. Bunlar; 1) Semantik, 2) Pragmatik 3) Kurumsal Mesleki yargı olmak üzere 3 türdür.

Semantik Mesleki Yargı: Kavramların anlamını ve dolayısıyla sınırlarını belirlemeye dönüktür. Daha çok kanun, tebliğ, yönetmelik vb. yasal düzenlemelerin yorumlanmasında karşılaşılır.

Pragmatik Mesleki Yargı: İki seçenekli durumdan birisine karar vermektir.

Kurumsal Mesleki Yargı: Düzenleyici kurumların başında yer alan kişilerin konuya bakış açılarını ifade etmek için kullanılır (Solaş,2006).

Muhasebe ve denetimde semantik ve pragmatik mesleki yargı türü kullanım alanı bulurken resmi veya gayri resmi kurum kuruluş ve örgüt yöneticileri düzeyinde daha çok kurumsal mesleki yargı söz konusu olmaktadır.

Muhasebe ve denetimde mesleki yargı sübjektiflikten uzak o mesleği icra edenlerin ve ilgili mesleki kuruluşların yasal düzenlemelerin hem fikir olduğu ve tarif ettiği bir çerçevede kullanılan bir yargıdır. Bu nedenle adı mesleki yargıdır. Başka deyişle “mesleki” kelimesi belli bir alana özgü teknik bilgiye sahip olma durumunu ifade eder. Buradan söz konusu teknik bilgiye sahip olmadan mesleki yargıda bulunulamayacağı sonucu çıkarılabilir.

Mesleki yargı sürecinin 4 temel bileşeni vardır (Dalkılıç, 2008). Bunlar;

1. Yargı gerektiren durum
2. Yargıda bulunan kişi ya da kişiler
3. Süreç
4. Çıktı (karar ve sonuçları)

Mesleki yargının bileşenleri epistemolojik açıdan irdelendiğinde; yargı gerektiren durum nesneye, yargıda bulunan kişi (muhasebeci, denetçi vb.) ise özneye karşılık gelmektedir. Bu durum aşağıdaki tabloda gösterilmiştir.

Tablo 1: Mesleki Yargıda Özne ve Nesne Bileşenleri

Mesleki Yargı Sürecinin Bileşenleri	Epistemolojik Karşılığı	Muhasebe ve Denetimdeki Karşılıkları
Yargı gerektiren durum	Nesne	Verilecek Karara İlişkin Seçeneklerin Her Biri <i>Örneğin, yasalar, standartlar vb. metinlerde yoruma açık fakat bir karar vermeyi gerektiren her olgu ve karar seçenekleri yargı gerektiren durumlar epistemolojik açıdan “nesne” konumundadır.</i>
Yargıda bulunan kişi ya da kişiler	Özne	Muhasebeci veya denetçi <i>Örneğin finansal tabloların hazırlanması sürecinde görev alanlar, muhasebe meslek mensupları ve finansal raporların denetimde yer alan herkes epistemolojik açıdan “özne” konumundadır.</i>
Süreç	Bilme Süreci	Değerlendirme ve Karar Süreci <i>Örneğin yoruma açık fakat karar verilmesi gereken bir durumda karar verirken izlenen yol ve yöntem (daha deneyimli meslektaşının uygulamasını benimseme, kendi deneyimlerini kullanma vb.) epistemolojik açıdan “bilme süreci” olarak adlandırılır.</i>
Çıktı (karar ve sonuçları)	Bilgi/Bilme	Karar

4. Bağımsız Denetimde Özne-Nesne İlişkisinin Mesleki Yargıya Etkileri

Yargıda bulunan kişinin deneyimi arttıkça mesleki yargının isabet derecesinin artacağı bilinen bir olgudur. Aynı zamanda mesleki yargının sürekli kullanımı deneyimlerini de artıracaktır. Çünkü yargı ve deneyim kazanma süreci (Kant'ın epistemoloji görüşüne uygun olarak) çift yönlü bir süreçtir. Meslek mensuplarının mesleklerinin ilk yıllarında daha çok kendinden öncekilerinin (muhasebe meslek mensupları arasında yaygın olarak kullanılan ifade ile: üstadlarının) yaptıklarını taklit ederken, ilerleyen yıllarda kendi görüş, düşünce ve deneyimlerini kullanarak karar vermeleri yargı-deneyim etkileşiminin bir sonucu olduğu söylenebilir.

Özne-nesne ilişkisinde birinin diğerine göre daha baskın olmasının muhasebe ve bağımsız denetimde mesleki yargı açısından bazı özel sonuçları ortaya çıkar. Bir denetçiden beklenen mesleki yargının ayırt edici özelliği, bu yargının, makul yargılara varmak için gerekli yetkinliği sağlayan eğitim, bilgi ve deneyime sahip bir denetçi tarafından yapılmış olmasıdır (BDS 200,p.A24). Bir durumda mesleki muhakemenin kullanılması, denetçi tarafından bilinen durum ve gerçeklere bağlıdır. Denetim sırasında ortaya çıkan zor veya ihtilafli konularda, örneğin BDS 220'nin p.15 gerektirdiği gibi, hem denetim ekibi içinde hem de denetim ekibi ile diğer kişiler (denetim şirketi içinden veya dışından uygun kademedeki kişiler) arasında istişare yapılması, denetçinin bilgiye dayalı ve makul yargılara varmasına yardımcı olur (BDS 200,p.A25). Mesleki muhakeme, varılan yargının, denetim ve muhasebe ilkelerinin yetkin bir şekilde uygulanmış olduğunu yansıtıp yansıtmadığına ve denetçi raporu tarihine kadar denetçi tarafından bilinen olay ve durumlar ışığında uygunluğuna ve tutarlılığına göre değerlendirilebilir (BDS 200,p.A26). Mesleki muhakemenin denetim boyunca kullanılması ve uygun bir biçimde belgelendirilmesi gerekir. Bu çerçevede denetçinin çalışma kâğıtlarını, denetim sırasında ortaya çıkan önemli hususlarla ilgili sonuçlara ulaşırken vardığı önemli mesleki yargıları, söz konusu denetimle hiçbir bağlantısı bulunmayan tecrübeli bir denetçinin anlayabilmesine olanak sağlayacak şekilde hazırlaması gerekir (BDS 200,p.A27).

Nesnenin özneye baskın olması durumunda meslek mensubunun herhangi bir durum karşısında verdiği karar sonrası sonuçları gözlemesi ve ders çıkarması benzer olayların tekrarında yargısını geliştirecektir. İnsanlar yargıda bulundukça tecrübe kazanmakta ve öğrenmektedir. Bu durum mesleki yargıda bulunma sürecinde nesnenin belirleyici olmasının sonucudur. Nesnenin belirleyici olmasının doğal sonucu benzer deneyime sahip meslek mensuplarının benzer mesleki yargılara varmasıdır. Nesnenin baskın olması durumunda bir süre sonra mesleki yargı da ortadan kalkacağı öngörülebilir.

Diğer taraftan bilme sürecinde bağlamın da belirleyici olduğunu öne süren bir görüş vardır. Özne nesne etkileşiminde (bilen ve bilinen yanında) bağlamın da belirleyici olduğu durumlar ortaya çıkabilir. Örneğin diğerlerine göre belirgin şekilde farklı sosyo-kültürel özellikleri olan meslek mensuplarından oluşanlarla sosyal ilişkiler kuranların bir süre sonra birbirine yakın yargılarda buldukları görülecektir. Bu durum da gösteriyor ki mesleki yargıda bağlam (içinde bulunulan sosyo-kültürel ortam) da belirleyici olmaktadır. Kant'ın

tam olarak ifade etmek istediği nokta burasıdır. Fakat gerek çevreden gerekse deneyimlerinden ders çıkarıp öğrenmenin hızı ve derecesi kişinin algı ve yeteneklerine bağlıdır. İşte bu noktada mesleki yargı sürecinde öznenin baskın hale geldiği, belirleyici olduğu görülür. Öznenin belirleyici olmasının doğal sonucu aynı konuda çok sayıda mesleki yargının ortaya çıkmasıdır. Böylesi bir sonucun zihinleri karıştıracığı aşıkardır.

5. Sonuç

Zaman zaman mesleki yargıda bulunma sürecinde özne veya nesneden birinin belirleyici olduğu farklı durumlar olabilmektedir. Diğer bir ifadeyle bazı durumlarda nesne, bazı durumlarda nesne belirleyici olmaktadır. Fakat kişinin dış dünyayı anlamlandırması yine kendi kişisel psiko-kültürel özelliklerinden etkilenmektedir. Bu noktada muhasebe ve denetimde mesleki yargıda bulunma sürecinde öznenin belirleyici olduğu söylenebilir. Bu durum muhasebe ve denetimde mesleki yargıda bulunma eyleminde Kantçı bakışın hakim olduğunu gösterir. Eğer Platoncu yaklaşım hakim olsaydı, mesleki yargı diye bir şey söz konusu olmazdı. Çünkü Platoncu yaklaşımda kişinin yargıda bulunmasına gerek yoktur, zaten kişi ne yapacağını biliyordur.

Mesleki yargıda nesne baskın olduğunda muhasebe uygulamalarının tekdüzeliğe doğru evrileceği öngörülebilir. Tekdüzelik meslek mensuplarını rahatlatan, bu nedenle arzu edilen bir sonuç olarak değerlendirilebilir fakat yaratıcılığı ve özgün uygulamaların ortaya çıkmasına katkı sağlamayan bir ortam oluşturacağı tehlikesini göz ardı etmemek gerekir. Özenin baskın olduğu ortamlarda ise aynı olay ve olgu hakkında birbirinden farklı, çok çeşitli yargılarla karşılaşmak beklenebilir.

Çıkar Çatışması

Yazar herhangi bir çıkar çatışması olmadığını bildirmiştir.

Finansal Destek

Yazar bu çalışma için herhangi bir kurum veya kuruluştan finansal destek almamıştır.

Hakem Değerlendirmesi

Dış bağımsız

Kaynakça

- BDS-200: Bağımsız Denetçinin Genel Amaçları ve Bağımsız Denetimin Bağımsız Denetim Standartlarına Uygun Olarak Yürütülmesi, www.kgk.gov.tr, 16.05.2021
- Dalkılıç, F.A., (2008). Mesleki yargı sürecinin muhasebe standartları kapsamında incelenmesi. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 10(3), 1-18.
- Göçmen, D., (2008). Özne felsefesinde iki dönüm noktası: Bazı güncel yaklaşımlar bağlamında René Descartes'tan Adam Smith'e öznenin kuruluşu ve kurtuluşu. *Baykuş*, 43-81.
- Öner, N., (2015). Bilginin serüveni, Divan Kitabevi, İstanbul.
- Simard, J., Claude (Çeviren Adıbelli, R.), (2003). "Epistemoloji", *Bilimname II*, Sayı 2, 13-21.
- Solaş, Ç., (2006). Muhasebe Mesleğinde Mesleki Yargı, Ders Notu, http://docs.google.com/View?id=ddmwd459_28f356dsfk 16.05.2021
- Sürmen, Y., Bayraktar, Y., (2015). Muhasebe ve denetim mesleğinde mesleki yargı kullanımının değerlendirilmesi: Borsa İstanbul (BIST) 100 endeksi'ndeki şirketler üzerine bir araştırma. *Muhasebe ve Finans Tarihi Araştırmaları Dergisi*, 9, 108-152
- Yıldırım, C., (2012). *Bilim Felsefesi*, Remzi Kitabevi, İstanbul.

Özgeçmiş

Selahattin KARABINAR: 1970 yılında Emet/Kütahya'da doğdu. 1992 Marmara Üniversitesi İİBF İşletme Bölümünden mezun oldu. Aynı kurumda 1994 yılında yüksek lisans eğitimini, 1998 yılında da doktora eğitimini tamamladı. Karadeniz Teknik Üniversitesi, Sakarya Üniversitesinde görev yaptı. Halen İstanbul Üniversitesi İktisat Fakültesi İşletme Bölümünde öğretim üyesi olarak görev yapmaktadır.

Case Study/Vaka Çalışması

USING BIG DATA IN INTERNAL FRAUD DETECTION

Teoman Samet TEMUÇİN¹Sefa ERBAŞ²Anıl AY³

Submitted/Başvuru: 28.06.2021

Last Revised/Son Düzeltme: 11.07.2021

Accepted/Kabul: 13.07.2021

Abstract

Internal frauds are one of the most important operational risks threatening entities. In addition to significant operational loss, they also cause reputational and prestige loss. Therefore, in addition to preventive proactive controls, existence of deterrent practices to quickly detect them is of great importance. In this paper, we will tell transformation story of Garanti BBVA Internal Audit Department regarding detection of internal frauds made through use of big data capabilities. We will talk about how the previous detection method called as “scenario-based” has been converted into the new one called as “rule-based” with more effective use of big data. This new detection method has allowed assurance to higher number of risky transactions with the same resources, achievement of significant increase rate in detection of internal frauds and decrease in the loss incurred due to internal frauds. We hope that this new methodology which has proven its success will also be a source of inspiration for the sector.

1 Dr., Internal Audit Manager, Garanti BBVA Internal Audit Department, e-mail: teomant@garantibbva.com.tr, ORCID ID: 0000-0001-7095-1686

2 Data Scientist, Garanti BBVA Internal Audit Department, e-mail: sefae@garantibbva.com.tr, ORCID ID: 0000-0002-1623-3664

3 Fraud Specialist, Garanti BBVA Internal Audit Department, e-mail: anilay2@garantibbva.com.tr, ORCID ID: 0000-0001-9612-3045

To cite this article: Temuçin, T. S., Erbaş, S., & Ay, A. (2021). Using Big Data in Internal Fraud Detection. *TIDE Academia Research*, 3(1), 55-84

Keywords: Internal fraud, Fraud detection, Big data

JEL Classification: C55, C8, K42, M42

İÇ SUIİSTİMALİN TESPİTİNDE BÜYÜK VERİNİN KULLANILMASI

Öz

İç suiistimler, kurumları tehdit eden en önemli operasyonel risklerden biridir. Verdikleri büyük operasyonel kayıplara ek olarak, kurumların itibar ve prestij kaybına da neden olmaktadır. Bu nedenle, söz konusu eylemleri önleyici proaktif kontrollerin varlığı kadar, hızlı bir şekilde tespit edilmesini sağlayacak caydırıcı uygulamaların da mevcudiyeti önem arz etmektedir. Bu makalemizde, Garanti BBVA Teftiş Kurulu Başkanlığı'nın büyük veri imkanlarını kullanarak iç suiistimalin tespitinde gerçekleştirdiği dönüşüm hikayesini paylaşıyor olacağız. “Senaryo bazlı” olarak nitelendirilen önceki tespit yaklaşımının, büyük veri imkanlarının daha etkin kullanılmasıyla “kural bazlı” olarak adlandırılan yeni tespit yaklaşımına dönüşümünden bahsedeceğiz. Söz konusu yaklaşımla; aynı kaynakla daha fazla riskli işleme güvence verebilmek, iç suiistimal tespit oranında ciddi bir artış oranına ulaşmak ve iç suiistimal nedeniyle karşılaşılabilecek kayıp tutarında da azalış yakalamak mümkün olmuştur. İç suiistimalin tespitinde başarısını kanıtlayan bu yeni yöntemin sektöre de ilham kaynağı olmasını umuyoruz.

Anahtar Kelimeler: İç suiistimal, Suiistimal tespiti, Büyük veri

JEL Sınıflandırması: C55, C8, K42, M42

1. Introduction

Operational risk is the probability of loss caused by processes, external events or information systems due to insufficient internal controls. As a more detailed definition, it is the probability of any loss or damage which may be caused by failure to detect mistakes and misconducts as a result of the problems in the internal controls, personnel's not acting in accordance with the conditions, errors and problems in the information systems, internal or external frauds, natural disasters or terrorist activities. (Babuşcu et al., 2018)

As can be understood from the definition, one of the most important factors causing operational risk is the personnel. This risk may be caused by unintentional mistakes, omissions or faults of the personnel as well as intentional actions such as embezzlement, gaining unjust benefits or stealing. These intentional actions are generally defined as "internal fraud". The major internal fraud cases seen in the banking sector are embezzlements and gaining unjust benefits. Embezzlements are generally committed by the personnel from the bank cash vault or from customer accounts by using forged documents. The unjust benefits, on the other hand, are gained by causing loss to the entity they work for by granting improper loans, leaking critical information outside, intentional pricing made against the entity's benefits and abusing one's powers based on agreements reached with internal/external stakeholders, and earning benefits from such losses.

This raises the question that why the personnel commit frauds at the entities that they work for. The answer to this question can be given with the "fraud triangle" in the literature. The fraud triangle framework indicates the factors which cause someone to commit internal fraud. It outlines three components which lead to fraudulent activity: opportunity, incentive (also known as pressure or motivation) and rationalization. (Figure 1)

Cressey's (1953) main hypothesis was that "Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-sharable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property."

Opportunity is any gap or control weakness on the system, which may facilitate the commitment of the fraud. Weak internal controls such as ineffective implementation of the principle of segregation of duties, the lack of an effective monitoring mechanism, a governance environment established on excessive trust, the lack of supervision and poor documentation of the processes create opportunities to commit internal frauds.

Incentive means the mindset or motivation of the personnel towards committing internal frauds. Indebtedness or greed of the personnel, luxurious living habits exceeding personnel income, illegal activities requiring high resources (gambling, drugs, etc.), sale pressure or unrealistic performance targets can be given as examples for motivation to commit frauds.

Rationalization refers to an individual's justification for committing fraud. At this point, the personnel firstly have to conclude that the return from the fraud will be higher than the loss to be incurred from the potential detection of the fraud. They also have to justify their actions based on grounds such as job dissatisfaction, the limited loss to be caused by the frauds and similar actions committed by other people.

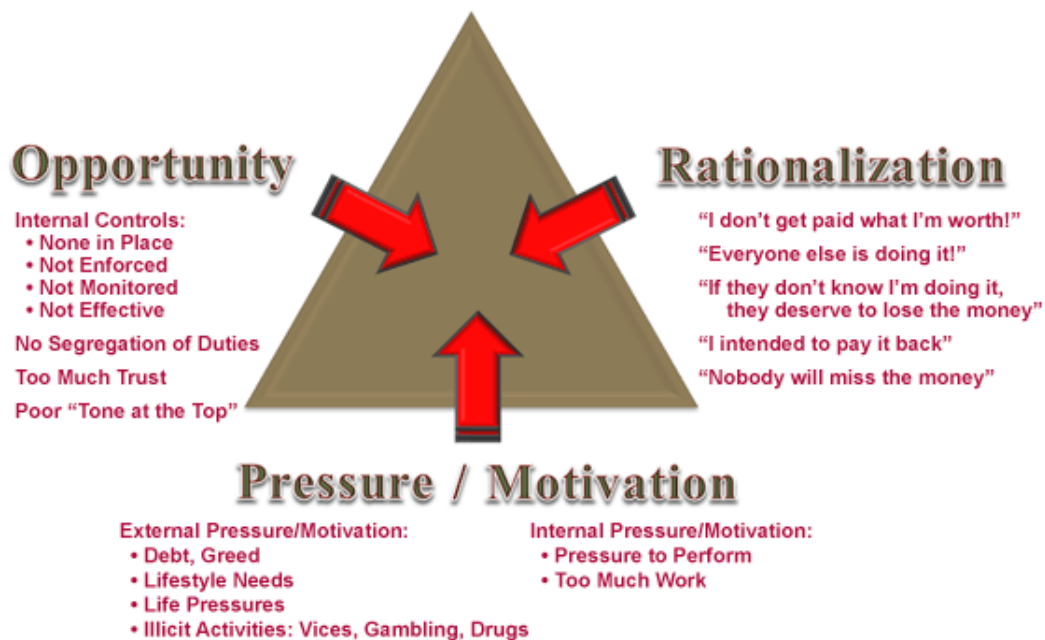


Figure 1: The Fraud Triangle
 Source: Association of Government Accountants (n.d.)

The presence of these factors causes fraud attempts by the personnel. Wolfe and Hermandson (2004) added a fourth factor “capability” to these three factors and named this new model “The Fraud Diamond”. Capability means that the fraudster should have certain personal traits (e.g. greed, weakness of character, excessive pride, dishonesty, etc.) and abilities (e.g. knowledge of processes and controls, etc.) to commit frauds.

In order to effectively manage the fraud risk, the entities have to prevent any environment/opportunity allowing internal frauds or to detect the committed frauds as soon as possible. Otherwise, frauds may cause loss of trust and reputation as well as high amounts of operational losses.

In terms of the banking sector in Turkey, the internal systems structures of the banks have a significant responsibility in terms of frauds. The Internal Control Unit, a member of the internal systems unit, may deprive the fraudsters the opportunity to commit frauds via strong proactive control points to be determined. The Internal Audit, on the other hand, can manage internal frauds effectively with strong processes to be recommended regarding the governance environment of the fraud and reactive periodical examinations to detect internal frauds.

In this paper, we plan to focus on the examination methods that can be used to detect internal frauds based on the factors in the fraud triangle. First, we will talk about the “scenario based” examination method that is implemented for long years at the entity we work for. Then, we will explain how “scenario based” examination has been converted into “rule based” examination method in 2019 Q4 with the more effective use of the big data. We will also explain how the internal fraud incidents will be detected more easily and effectively in terms of quality and efficiency with the “rule based” examination method implemented by using big data capabilities. We aim that this new examination methodology used to detect internal frauds by using big data capabilities will shed light on the sector regarding internal fraud detection.

The paper is organized as follows: Section 2 provides a literature review of the internal fraud prevention and detection methodologies. Section 3 explains the previous internal fraud detection approach in Garanti BBVA and how it is integrated into a new meth-

odology by using big data capabilities. Section 4 presents the comparative results of two applied methodologies and inspires readers for applying a similar approach and finally, Section 5 provides a conclusion on the subject.

2. Literature Review

Entities can protect themselves from major internal frauds only with continuous efforts and practices supporting each other. The main practices in this respect can be categorized into two as proactive and reactive.

2.1. Proactive Practices

Proactive practices include deterrent and preventive practices to prevent internal fraud incidents from happening. These controls aim for minimizing the “opportunity” factor under the fraud triangle to the maximum extent possible and not providing the personnel who may plan to commit a fraud with the actual opportunity to do so. The establishment of an effective fraud risk governance and regular fraud risk assessments are of critical importance for this process. After the establishment of a proper fraud risk governance environment, optimal deterrent and preventive controls are expected to be established on the weak points with regular risk assessments.

Fraud risk governance refers to existence of a detailed anti-fraud policy and written responsibilities of board of directors and top management regarding fraud risk management. The lack of an effective governance environment or the highest level of tolerance by the entity regarding internal frauds weaken the effective management of the internal fraud risk. Roles and responsibilities, expectancies from each level of employee within the anti-fraud policy, fraud risk assessment approach, establishment of deterrent and preventive controls, continuous monitoring and detection and inspection/investigation processes should be defined under fraud risk management program.

Fraud risk assessment is the definition of potential internal fraud activities at the entity and preparation of an impact/probability matrix for them. In order to protect themselves against internal frauds, the entities must first understand and define fraud risk. Then, they have to periodically evaluate the areas where these defined risks may be experienced depending on their activities, size, working method and goals.

The next step is the foundation of effective deterrent and preventive controls after the riskiest areas are determined within the fraud risk assessment process. Prevention covers any type of policy, procedure, training, and communication which will prevent frauds. Deterrence, on the other hand, is raising awareness among the personnel that effective detective practices and continuous fraud monitoring process are available. According to the Application Paper of International Association of Insurance Supervisors (2011), some of the examples of deterrent and preventive controls are listed below:

- *establishing clear responsibilities in documented job descriptions or role statements,*
- *requiring periodical job rotation and mandatory vacations for management and staff in fraud sensitive positions,*
- *eliminating potential conflicts of interest between ... (the related parties),*
- *separating or dividing any function that may cause or be susceptible to conflicts of interest,*
- *adequate segregation of functions,*
- *establishing efficient physical and procedural safeguards over the use, handling and availability of cash, other assets, and transactions as well as of information systems,*
- *arranging for cash and money flows to be dealt with by more than one person,*
- *establishing internal complaints procedures for disgruntled management and staff,*
- *establishing a clear dismissal policy for internal fraud cases in order to deter other potential perpetrators. etc. (p. 10)*

If these controls are supported by organizing trainings for and raising awareness of the personnel about internal frauds and informing them about reward and whistleblowing practices with a strong anti-fraud policy, effective proactive practices will be established at the entity.

2.2. Reactive Practices

Proactive practices are not sufficient alone to prevent internal frauds. As we have mentioned above, proactive applications minimize the “opportunity” factor on the fraud triangle while reactive applications focus on the “rationalization” factor. Rationalization is the conclusion by the personnel that the return from the fraud will be higher than the loss to be incurred in case of potential detection of the fraud. Thus, the existence of effective reactive practices and availability of internal fraud detection tools increase the potential to detect frauds and decrease the rationality of the personnel to commit frauds.

Reactive practices are any type of methods that allow detection of an internal fraud on time (as soon as possible). The early detection of an internal fraud is important to minimize the operational loss and reputational risk that may be caused by the fraud. “Consequently, quick detection of fraud is vital to protecting an organization from potential damage. ... the longer a fraud remains undetected, the greater the financial losses.” (Association of Certified Fraud Examiners [ACFE], 2020, p. 14)

The strong internal fraud detection approaches are mainly created by three considerations. The first is to determine the areas/works prone to frauds due to the control deficiencies with the fraud risk assessment. The second is to put oneself into the shoes of the personnel committing frauds and to consider the frauds that they may commit in the areas with control deficiencies. The last is to utilize big data capabilities based on the anomalies and patterns determined in the first two steps and to regularly examine the similar transactions (continuous risk monitoring).

In summary, deterrent/preventive controls aim for preventing frauds while detection aims for detecting fraud as soon as possible. Therefore, the implementation of the optimal combination of both practices is the correct approach for the effective management of the internal frauds. (ACFE, 2008)

2.3. The Role of Internal Audit

According to the Institute of Internal Auditors (IIA) definition, internal auditing is an in-

dependent, objective assurance and consulting activity that aims to add value and improve an organization's operations. Therefore, the internal audit has some roles and responsibilities in order to minimize the fraud risk for improving the operations of the organization. When we review the IIA's standards (IIA, 2017), we encounter following responsibilities regarding fraud risk.

- 1210.A2 – *Internal auditors must have sufficient knowledge to evaluate the risk of fraud.* (p. 6)
- 1220.A1 – *Internal auditors must exercise due professional care by considering the ... probability of significant errors, fraud, or noncompliance.* (p. 7)
- 2120.A2 – *The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.* (p. 14)
- 2210.A2 – *Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.* (p. 15)

Accordingly, internal auditors should have relevant skills for evaluating fraud risk, exercise due professional care by considering the fraudulent activities and evaluate fraud risks while developing the objectives of the audit engagements. Therefore, the internal audit activity should take into consideration fraud risk exposures and management of them. When we combine these expectations and standards with the sections above, we reach the following conclusion: the internal audit may have an advisory role for setting proactive practices and may also undertake a direct responsibility regarding internal fraud detection based on its independence and objectivity role (reactive practices). In fact, according to the ACFE's Report to the Nations (2020), "internal audit" is considered to be the second most successful in fraud detection after "tips and whistleblowing".

In parallel with this conclusion, according to the IIA's Position Paper (2019), internal audit should evaluate proactive controls taken by the organizations in order to limit fraud risk. The fraud risk and adequacy of anti-fraud controls should be included under the scope of all relevant audit engagements. Besides, "internal audit's role includes detecting,

preventing, and monitoring fraud risks and addressing those risks in audits and investigations.” (p. 2) based on the definition of internal auditing. According to the IIA’s perspective, investigation is not typically an internal audit task. However, if internal audit is required to investigate fraud and the internal auditors have the necessary skills and experience, then investigation activities could be performed by the internal audit as well.

In fact, considering internal audit’s being independent and objective, after the detection of the internal fraud, it is reasonable that the inspection and investigation activities could be carried out by the internal audit by maintaining confidentiality. We are of the opinion that since the internal audit reports directly to the board of directors, the internal audit can duly undertake the following roles if it has experience and skills in the field of frauds:

- To reveal the nature of and loss caused by internal frauds with investigations,
- To evaluate the risks that may be incurred due to the frauds (operational, legal and reputation),
- To make recommendations to the related units to take corrective actions,
- To provide guidance together with the human resources department to take disciplinary actions.

2.4. Modern Detection Techniques

We have discussed the need for both proactive and reactive practices in order to manage fraud risk effectively. Under the reactive practices section, we have mentioned that the quick detection of fraud is critical for the minimization of operational loss and reputational risk. In this section, we will now focus on the “capability” factor under “The Fraud Diamond” model.

We have defined capability as the fraudster’s having certain personal traits (e.g. greed, weakness of character, excessive pride, dishonesty, etc.) and abilities (e.g. knowledge of processes and controls, etc.) to commit frauds. At this point, we have to put ourselves in the shoes for the personnel committing frauds and think about the capabilities of the personnel and how they will commit frauds in the areas of the entity with control weakness-

es for designing an effective detection methodology. We are then expected to determine potential frauds and regularly examine them based on the anomalies and patterns to be determined with this perspective and by using big data capabilities.

Therefore, the most critical question regarding detection is how to determine the sample transactions based on the anomalies and patterns defined among thousands of transactions (audit population)? The most critical factor for the success of the entities regarding detection is whether they utilize the big data capabilities effectively or not.

The literature also focuses on visualization of the data and modelling of fraud incidents by utilizing big data capabilities for effective fraud detection. (Fawcett and Provost, 1997; Rosset et al., 1999; Bolton and Hand, 2002; Becker et al., 2010) According to Baesens et al. (2015), “big data and analytics provide powerful tools that may improve an organization’s fraud detection system.”

The literature goes one step beyond of detection of anomalies by using big data capabilities and their modelling and recently focuses on how to use machine learning for fraud detection. (Baesens et al., 2021; Wei et al., 2020; Ge et al., 2020; Kolodiziev et al., 2020; Shirgave et al., 2019; Soviany, 2018)

All these articles agree on that determining a sample including the risky transactions (with the highest internal fraud risk) by effective adaptation of data mining and the identified anomalies/patterns to the available data. The next step is to use machine learning and to minimize manual intervention and automatic update of the rules by using the accumulated “proven fraud” and “false positives” with a statistical model to be selected. In summary, the use of big data capabilities and machine learning aims for effectively determining the transactions with the highest fraud potential (an effective sample).

Therefore, as big data is the most valuable asset today, it would be illogical not to use this opportunity to detect internal frauds. Garanti BBVA Internal Audit Department launched a new project in 2019 Q4 on how we can effectively use big data capabilities for the detection of internal frauds. As a result of this project and using big data more effectively, we have started to use the “rule based” examination methodology instead of the “scenario based” examination method that we have been using for years. This new detec-

tion method that we will provide detailed information about its contents and results in the following sections has allowed us to create a more efficient and effective sample pool by using big data as explained under the literature. The results that we have achieved regarding internal fraud detection in 2020 support our arguments regarding our new detection method. Another advantage of this methodology is that the “proven fraud” and “false positives” data being accumulated day by day will help us to integrate machine learning to our system in near future.

3. Methodology and Data

3.1. Methodology

Internal frauds are the intentional actions committed by any individual authorized to carry out transactions at an entity by displaying deceitful behaviors to gain benefits. The most common internal fraud method in banking is the embezzlement of the customer money by the personnel by using various methods without the knowledge of the customers.

The most risky channel in terms of commitment of internal frauds is the bank branches since no intervention can be made to the transactions carried out on alternative distribution channels, confirmations are obtained from the customers upon performing transactions on their behalf (customer signature on the transaction receipt) and the transactions performed are under the initiative of the personnel. Taking this into consideration, for the internal fraud detection, the transactions performed via the branches should be included in the examination scope. Moreover, the embezzlement of the money as part of an internal fraud activity is made by taking the money physically (money withdrawal) or its electronic transfer (money transfer).

In line with all this information, all money withdrawal and transfer transactions performed via the Bank⁴ branches constitute the audit population of an internal fraud detection system based on risk scoring.

⁴ The Bank refers to Garanti BBVA.

3.1.1. Former Approach (Scenario-based)

The scenario-based examination method has been used to detect internal frauds before the project implementation (before 2019 Q4) and examinations have been carried out based on 25 different scenarios in average.

These scenarios have been prepared by taking into consideration the expert opinions and inspection reports in the light of the previous internal fraud cases at the Bank and/or in the sector. Even though scenarios have been designed to determine whether the transactions performed are fraudulent, they only reflect the intersection set of a few risk factors (rules) that they include and therefore, focus on just a few risk points at the same time.

For instance, in the scenario named “customers who do not have a digital banking product and are over a certain age”, the transactions which satisfy both criteria are included in the examination sample. However, regardless of the age of a customer, not owning any digital product and therefore, having a low capability to control his accounts on a real time basis is a risk but such customers are not included in the sample based on this scenario.

Moreover, the data regarding these scenarios are obtained by the auditor from different channels (Structured Query Language [SQL], SAP, the Banking applications, etc.) before the examination and especially obtaining data with these complex methods renders the process prone to manual interventions and causes waste of time and thus, inefficiency.

The examination frequency of these scenarios has been designed as monthly, bimonthly, quarterly, semi-annually, or annually depending on the determined risk of the scenario. This causes the examination of transactions under some scenarios after a very long time upon their performance and thus, delays in the detection of a potential fraud. In other words, a fraud may not be detected for 1 year.

Moreover, while performing scenario-based examinations, the auditor examines all risky transactions under the same scenario and this may cause audit blindness (audit risk) on the auditor from time to time.

In conclusion, the scenario-based examination method had areas of improvement regarding design and efficiency even though it has enabled us to make important detections.

3.1.2. Current Approach (Rule-based)

The “scenario-based” approach has been replaced by the “rule-based” approach with the more effective use of the big data capabilities and a data project carried out in 2019 Q4. The sub-risk factors (rules) constituting each scenario under the scenario-based examinations are examined separately and together under rule-based examinations. All risk rules that will support the suspicion that the customer is not aware of the transactions performed on the accounts are obtained from the scenarios. These risk rules can be grouped under 3 main elements of the transactions examined under the project.

The 3 main elements of the money withdrawals and money transfers made from the Bank branches are as follows:

- **Personnel:** The personnel who performs the suspicious transactions.
- **Customer:** The Bank customer who is a party to the relevant transaction.
- **Transaction:** The features of the transactions changing depending on the transaction amount, performance time, subject, etc.

Some examples regarding the rule sets matching with the risk factors grouped under the related elements are presented below in order to help you visualize them better:

Risky Personnel: High indebtedness of the personnel, high number of transactions performed by the personnel for the same customers, betting and illegal actions identified, working for a long time at the same branch etc. can be given as example.

Risky Customer: Not having any digital channel product (mobile banking, internet banking), having an address of residence abroad or being a foreigner, personnel’s viewing his accounts and/or other products on the Core Banking application more frequently than

the normal viewing level, no branch q-matic queue number available for the day when a transaction is performed on the customer's behalf etc. can be given as example.

Risky Transaction: Performance of the transaction from an account that the customer does not use actively, not scanning the receipt into the system after its signing by the customer, the capability of performing transactions on time deposit accounts before account maturity date can be given as example.

More than 50 risk factors have been determined under the sub-elements (under risky personnel - risky customer - risky transaction categories) of the examined transactions and a score has been assigned to them depending on their risk level under the rule-based approach. This score assignment has been made by the Internal Fraud team of Garanti BBVA Internal Audit Department by taking into consideration previous experience and incidence frequency. Moreover, the risk level of the transactions is continuously examined and the scores of these risk factors are updated.

The entire process (*retrieval of the relevant data from Bank database, their categorization under sub-elements and creating of risk rule sets, assignment of a risk score for each rule set, matching the sub-elements for which risk score assignment is made with all transactions and creation of the examination sample based on final risk scoring*) has been designed on SQL environment from end-to-end and automatically starts every day with the support of the big data capabilities.

The designed system determines for each money withdrawal and money transfer transaction (audit population) which risk factors the transaction includes and assigns to that transaction the current scoring based on these factors. The scores for the risk factors that the transactions are tagged with are added up and the final risk score is assigned for each transaction. Therefore, all transactions in the audit population are scored based on the potential risk levels under the pre-determined rule set and are ranked based on the highest total risk point. Each day is designed as obtaining the data regarding all money withdrawal and transfer transactions performed through the branches on the previous day, processing them based on the pre-determined rule set and generating results.

Figure 2 shows how the process functions every day under three headings (Input - Data Processing - Output). Basically, the entire raw data are obtained from the Bank datawarehouse (DWH) environment and the customers, personnel and transactions matched with risk factors are determined and a separate risk pool is created. In the last step, the transactions performed on the previous day and the customers and personnel taking part in these transactions are matched with the information available in the risk pool and the final examination sample is created based on the highest risk score.

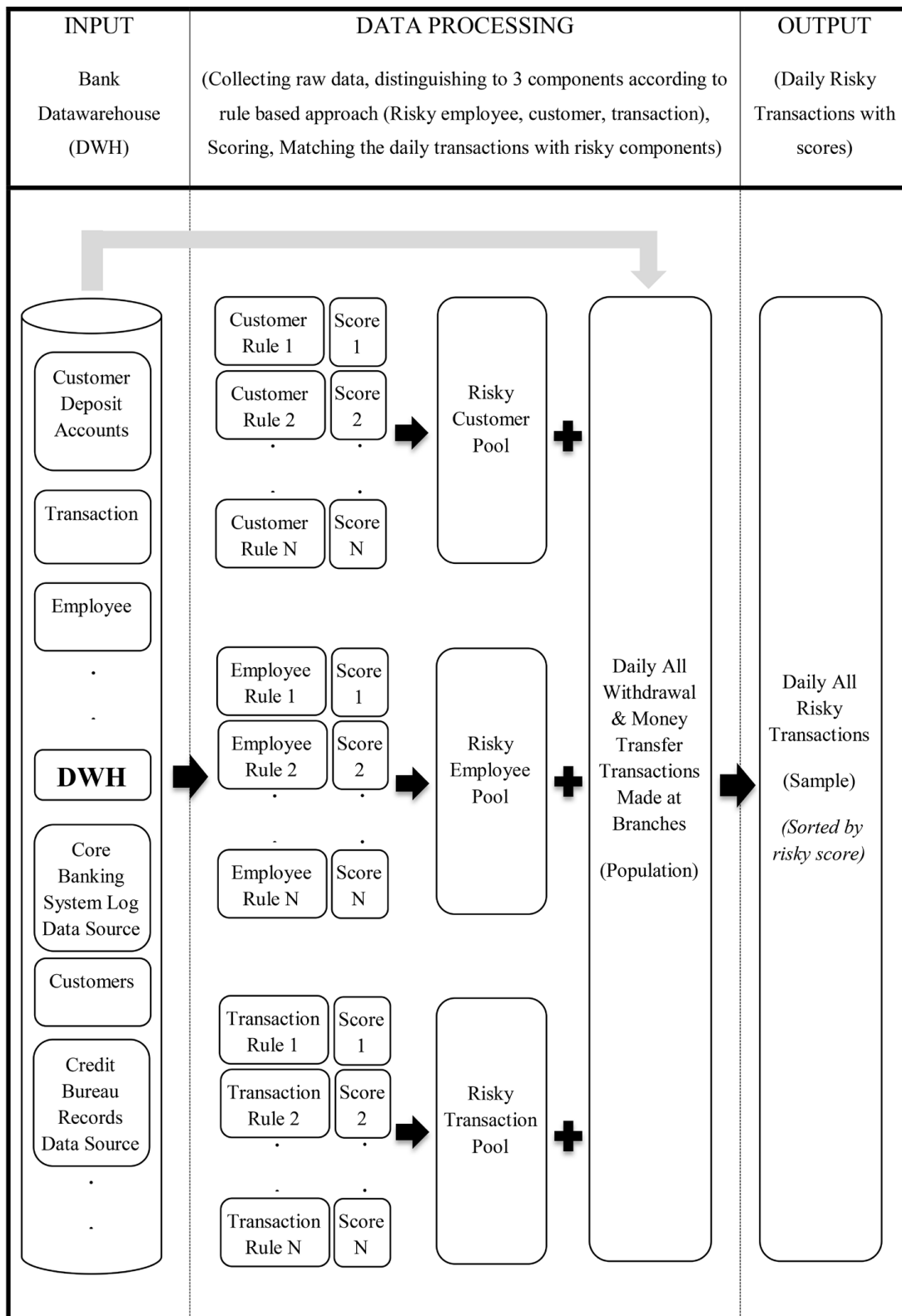


Figure 2: System Working Principle

3.2. Data

A high number of data resources are available in the Bank database and used in the determination of the defined risk factors within the scope of the Project. Some of these data resources and the main information they include are presented below as example.

Transaction: The data resource where all transactions performed by the Bank are recorded. It includes information on customers, transaction type, channel, date, time and amount of the transaction, transaction status (*cancellation or active*) or personnel performing the transaction. The money withdrawal and transfer transactions performed via branches are selected daily from among all transactions to create the audit population.

Employee: The data resource including the date of hiring, the branch where s/he works, the date for starting to work at the last branch, position, leaves used, title etc. information of the Bank employees.

Customer: The data resource including the demographic information, the branch where s/he gets service, digital channel (mobile, internet etc.) active use etc. details of the Bank customers.

Core Banking System Logs: The data resources where the logs of all transactions performed by the personnel on the core Banking application are kept. This data resource is especially used for the details of viewing of the assets and information of the customers by the personnel.

Branch Q-matic Transactions: The data resource including the date, time and transaction type of the queue numbers taken by the customer from the branch q-matics.

Customer Deposit Accounts: The data resource including the balance, type, maturity date for time deposit accounts and active use details for the deposit accounts of the customers.

Credit Bureau Records: The data resource including the details of active or passive loan and credit cards of the personnel at all banks.

The system matches the above sample information with the money withdrawal and trans-

fer transactions performed from the branches in line with the rules defined and assigns a risk score for each transaction in the audit population. For detection of internal frauds, the transactions with the highest risk scores are included in the sample and examined.

4. Comparison of Results

Comparisons are made between the pre-project (scenario-based) and post-project (rule-based) approaches of Garanti BBVA Internal Audit Department in terms of efficiency, internal fraud detection ratio and amounts of the Bank loss caused by internal frauds by using the project launched in 2020 as a reference point. According to the results of the comparisons made, the new approach implemented by using big data (rule-based) are more effective and efficient.

4.1. Efficiency

Before the implementation of the project within the scope of scenario-based examinations, the auditors used to obtain the data from different channels and make manual interventions frequently in order to obtain the final sample.

With the implementation of the new project (rule-based), obtaining the final sample is automatized and the data are obtained daily from a single channel without manual intervention. This has allowed allocation of nearly the entire labor force to the transaction examination and this has caused an increase of 25% in the number of examinations even though the labor force remained similar. (Table 1)

Table 1: Number of Total Transactions Examined (2019-2020)

Year	Number of Transaction
2019	24,677
2020	30,903

Moreover, even though it has been projected to examine 50,000 transactions in total in

2020 with the same labor force, a smaller number of transactions than the projected number has been examined due to the pandemic conditions. In summary, if similar conditions had been present in 2020 as compared to the previous year (under normal conditions), the number of transactions for which assurance has been provided with the same labor force would have been nearly doubled.

4.2. Internal Fraud Detection Ratio

According to the ACFE's Report to the Nations (2020), 43% of the internal frauds are detected via whistleblowing while 15% are detected by internal audit. (Table 2)

Table 2: How is Occupational Fraud Initially Detected?

Type	Ratio
Tip	43%
Internal Audit	15%
Management Review	12%
Other	6%
By Accident	5%
Account Reconciliation	4%
External Audit	4%
Document Examination	3%
Surveillance/Monitoring	3%
Notified by Law Enforcement	2%
IT Controls	2%
Confession	1%

Source: ACFE (2020)

Before the implementation of the project, the average internal fraud detection ratio for the Internal Audit Department was 21% in average for the internal frauds committed at Garanti BBVA and was parallel to the abovementioned ratio given by ACFE.

With the implementation of the project, the new method replacing the method of evaluating transactions with only a few rules under a scenario-based in the past has enabled the determination of a sample covering more risky transactions with the evaluation of a transaction with more than 50 rules.

Unlike the previous methodology, the daily examination of these transactions instead of monthly, quarterly, semi-annual or annual periodical examinations has allowed the evaluation of the transactions as fast as possible without the loss of the evidence regarding the transactions. This has resulted in a more effective sample examination and an increase in the capability of detection of frauds regarding the examined transaction. Moreover, the examination of different types of suspicious transactions determined with different rules instead of the examination of similar transactions under a single scenario has minimized the audit blindness (audit risk) to the minimum level.

Taking all the foregoing into consideration, the use of the new rule-based examination method has increased the average of detection of internal frauds by the Internal Audit Department by 119% in 2020. (Table 3) This is the clearest proof that the new method using big data capabilities is a more effective detection approach.

Table 3: Internal Fraud Detection Ratio (2016-2020)

Year	Average Detection Ratio
2016-2019	21%
2020	46%

4.3. Bank Losses Caused by Internal Frauds

Finally, as you can remember, we have discussed that the quick detection of frauds is critical for minimizing the losses to minimum. (ACFE, 2020)

Before the project, the examinations used to cover transactions dating back to one month at the earliest and transactions performed one year ago were examined in some cases depending on the examination period. The implemented project has enabled the examination of the transactions performed one day ago and also allowed the earlier identification of the fraudster and minimization of the loss.

In this respect, taking into consideration the average losses of the Bank incurred due to internal frauds, the internal fraud loss amount has decreased by 30% as compared to previous years. (Table 4)

Table 4: Bank Loss Caused by Internal Fraud (2016-2020)

Year	App. Loss Amount (EUR)
2016-2019	1,000,000
2020	700,000

In conclusion, the comparison of the above figures in several perspectives reveals that the rule-based internal fraud detection approach launched with the use of big data capabilities:

- has increased efficiency by allowing more examinations with the same resources,
- has caused a significant increase in the fraud detection ratio as a result of the examination of riskier transaction pool (sample) and
- has allowed earlier detection of the frauds as a result of the examinations of transactions in a short period of time and this has decreased the loss amounts.

5. Conclusion

Operational risk is the probability of loss caused by processes, external events or information systems due to insufficient internal controls. Therefore, one of the important operational risk resources at the banks is the internal frauds that may be committed by the personnel such as embezzlements, gaining unjust benefits, stealing etc. Internal frauds committed by the personnel cause operational losses as well as reputational and prestige loss for the entity. The factors causing the personnel to commit frauds are defined as opportunity, incentive, rationalization, and capabilities in the literature. Thus, the internal frauds causing operational and reputational losses at the entities can be minimized with the actions developed based on these factors.

The proactive practices used for this purpose are designed to minimize the “opportunity” factor to the best extent and not to give any opportunity to the personnel that may commit frauds while reactive practices focus on the “rationalization” factor and increase deterrence by reminding the personnel that the probability of detection is high. Moreover, effective fraud detection methods being the most common reactive practices are designed by taking into consideration the “capabilities” of the personnel. The potential frauds have to be detected based on the anomalies and patterns to be determined with this perspective and by using big data capabilities and regularly examined.

This paper focuses on effective detection methodology which can be used to detect internal frauds based on the defined rules. In this respect, the change made in the detection approach of Garanti BBVA by using big data capabilities is explained. First, information is provided on how the “scenario-based” examination method implemented at Garanti BBVA for years has been converted into the “rule-based” detection method with the effective use of big data capabilities.

The rule-based method replacing the scenario-based method where transactions are examined based on only a few rules under a scenario has allowed the simultaneous assessment of more than 50 rule sets and creation of a riskier transaction pool. This method has been achieved only with the effective use and management of the big data.

We conclude that the rule-based examination methodology implemented by using big

data capabilities allows efficient and effective way of detecting internal frauds. The rule-based internal fraud detection approach has enabled provision of assurance for more transactions with the same resource, a dramatic increase in the fraud detection ratio by determining a riskier transaction pool (sample) and less loss amount due to earlier detection of frauds with a shorter examination time period. We believe that this new examination method used to detect internal frauds by using big data capabilities will shed light on the sector regarding internal fraud detection.

The advantages of using big data in internal fraud detection are not limited to only the ones mentioned above and the use of a system focusing entirely on data allows accumulation of “proven fraud” and “false positives” data. In the sample pool, which is examined every day, the “proven fraud” represents the transactions which are decided to be internal frauds according to examination results while “false positives” are the transactions which are concluded not to be internal frauds. The accumulated data will allow integration of machine learning into the system for internal fraud detection as a next step, which is a future research interest for the authors.

Author Contribution

The authors have equal contribution to the paper.

Conflict of Interest

There is no conflict of interest among the authors.

Financial Support

The authors have not received any financial support for this study.

Peer-Review

Externally peer-reviewed

Acknowledgments

The authors would like to express their sincere gratitude to Osman Bahri TURGUT, CAE of Garanti BBVA, for his support and vision for continuous development and progress.

References

Association of Certified Fraud Examiners (ACFE), Institute of Internal Auditors, & American Institute of Certified Public Accountants. (2008). *Managing the business risk of fraud: A practical guide*. Association of Certified Fraud Examiners.

Association of Certified Fraud Examiners (ACFE). (2020) Report to the nations: 2020 global study on occupational fraud and abuse. Retrieved from <https://www.acfe.com/report-to-the-nations/2020/>

Association of Government Accountants (AGA). (n.d.). The fraud triangle. Retrieved from <https://www.agacgfm.org/Intergov/Fraud-Prevention/Fraud-Awareness-Mitigation/Fraud-Triangle.aspx>

Babuşcu, S., Hazar, A., & Iskender, A. (2018). *Banka risk yönetimi: Basel I - II - III - IV düzenlemeleri*. Bankacılık Akademisi Yayınları.

Baesens, B., Vlasselaer, V., & Verbeke, W. (2015). *Fraud analytics using descriptive, predictive, and social network techniques: A guide to data science for fraud detection*. Wiley Publishing.

Baesens, B., Höppner, S., & Verdonck, T. (2021). *Data Engineering for Fraud Detection*, Decision Support Systems, 113492.

Becker, R., Volinsky, C., & Wilks, A. (2010). Fraud detection in telecommunications: history and lessons learned. *Technometrics*, 52(1), 20-33.

Bolton, R. & Hand, D. (2002). Statistical fraud detection: A review. *Statistical Science*, 17(3), 235-255.

Cressey, D. R. (1953). *Other People's Money: A study in the social psychology of embezzlement*. Free Press.

Fawcett, T. & Provost, F. (1997). Adaptive fraud detection. *Data Mining and Knowledge Discovery*, 1(3), 291-316.

Ge, D., Gu, J., Chang, S., & Cai, J. (2020). Credit card fraud detection using lightgbm model. *International Conference on E-Commerce and Internet Technology*, 232-236.

International Association of Insurance Supervisors (IAIS). (2011, September 28). *Application paper on deterring, preventing, detecting, reporting and remedying fraud in insurance*. Retrieved from <https://iaisweb.org/file/34108/application-paper-on-fraud-in-insurance>

Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I., & Lozynska, O. (2020). Automatic machine learning algorithms for fraud detection in digital payment systems. *Eastern-European Journal of Enterprise Technologies*, 5(107), 14–26.

Rosset, S., Murad, U., Neumann, E., Idan, Y., & Pinkas, G. (1999). Discovery of fraud rules for telecommunications - challenges and solutions. *Proceedings of the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, NY: ACM Press, 409-413.

Shirgave, S. K., Awati, C. J., More, R., & Patil, S. S. (2019). a review on credit card fraud detection using machine learning. *International Journal of Scientific and Technology Research*, 8(10), 1217-1220.

Soviany, C. (2018). the benefits of using artificial intelligence in payment fraud detection: A case study. *Journal of Payments Strategy and Systems*, 12(2), 102-110.

The Institute of Internal Auditors (IIA), (2017, January 1). International standards for the professional practice of internal auditing (standards). Retrieved from <https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards.aspx>

The Institute of Internal Auditors (IIA), (2019, January). Fraud and internal audit: Assurance over fraud controls fundamental to success. Retrieved from <https://na.theiia.org/about-ia/PublicDocuments/Fraud-and-Internal-Audit.pdf>

Wei, Y., Qi, Y., Ma Q., Liu Z., Shen C., & Fang C. (2020). Fraud detection by machine learning, 2nd International Conference on Machine Learning, Big Data and Business Intelligence, 101-115.

Wolfe, D. & Hermanson, D. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal* 74.12, 38-42.

Resume

Teoman Samet TEMUÇİN, is Internal Audit Manager at Garanti BBVA. Experienced and skilled mainly in Capital, Market, Structural, Business Model and Operational (internal fraud, investigation and branch audits) risks. In addition to job functions, he holds a Ph.D. in Banking and Finance and contributed to various teaching and research activities.

Sefa ERBAŞ, is Data Scientist at Garanti BBVA Internal Audit Department. He graduated from Hacettepe University with bachelor's degree in business administration and also had master degree in Big Data Analytics. Experienced on modeling and advanced data analytics in various audit projects.

Anıl AY, is Fraud Specialist at Garanti BBVA Internal Audit Department. He graduated from Middle East Technical University with bachelor's degree in economics. He has had 5-year experience in internal fraud team.

Research Article/Araştırma Makalesi

COVID-19 KRİZİNDE SÜRDÜRÜLEBİLİRLİK PERFORMANSI VE ANORMAL PAY GETİRİSİ

Emrah KELEŞ¹

Submitted/Başvuru: 17.06.2021

Last Revised/Son Düzeltme: 17.07.2021

Accepted/Kabul: 18.07.2021

Öz

Bu çalışmada sürdürülebilirlik performansının pay performansı üzerine etkisi araştırılmaktadır. Çalışmada BIST Sürdürülebilirlik Endeksine dahil olan ve olmayan BİST 30 firmalarına odaklanılmaktadır. Bu firmaların anormal pay getirilerinin karşılaştırılması için olay çalışması yönteminden yararlanılmıştır. Çalışma kapsamında Covid-19 krizinde önemli tarihler – ilk vaka, ilk tedbirler ve ilk ölüm – dikkate alınmış ve incelenmiştir. Çalışma sonuçları BIST Sürdürülebilirlik Endeksine dahil olan firmaların kayıplarının olmayanlara göre daha az olduğunu göstermektedir. Bu da krizin ortaya çıkış dönemi sırasında yatırımcıların firmaların sürdürülebilirlik performanslarını dikkate aldığını ortaya koymaktadır.

Anahtar Kelimeler: Covid-19, sürdürülebilirlik, BİST, olay çalışması, kriz

JEL Sınıflandırması: G14, G15, M14

¹ Dr. Öğr. Üyesi, Marmara Üniversitesi, İşletme Bölümü, Muhasebe-Finansman Anabilim Dalı / Misafir Araştırmacı, WU Vienna University of Economics and Business, Institute for Finance, Banking and Insurance, emrah.keles@marmara.edu.tr, ORCID ID: 0000-0003-3840-277X.

To cite this article: Keleş, E. (2021). COVID-19 Krizinde Sürdürülebilirlik Performansı ve Anormal Pay Getirisi. *TIDE Academia Research*, 3(1), 85-104

SUSTAINABILITY PERFORMANCE AND ABNORMAL STOCK RETURNS DURING THE COVID-19 CRISES

Abstract

This study examines the effect of sustainability performance on financial performance. Specifically, this paper focuses on BIST 30 firms included and excluded in the Istanbul Stock Exchange BIST Sustainability Index. The event study methodology is applied to compare the abnormal stock returns for these firms. Three critical days – first case, first measures, first death – during the Covid-19 crisis are considered and investigated. The results show that firms included in the BIST Sustainability Index experience fewer loss comparing to the excluded ones, suggesting that investors value firms' sustainability performance during the crisis outbreak period.

Keywords: Covid-19, sustainability, BIST, event study, crisis

JEL Classification: G14, G15, M14

Extended Abstract

The emergence and rapid spread of the corona virus caused a shock effect on the society as well as on the financial markets. Particularly, it triggered tremendous heterogenous stock market reactions (Ding, Levine, Lin, & Xie, 2020). In addition to this, the effects of the corona virus pandemic have also started to be investigated rapidly and related studies have deepened and increased over time. In this context, it emerges as a subject that is emphasized both in theory and in practice, especially the financial effects are of interest.

Although current studies agree on the negative impacts, it seeks to answer the question about the conditions under which companies are more affected by this negative impact and how they can be protected from such shocks (Alfaro, Chari, Greenland, & Schott, 2020; Fahlenbrach, Rageth, & Stulz, 2020; Ramelli & Wagner, 2020; Zechner, Pagano, & Wagner, 2020). Since the Covid-19 crisis is an unexpected shock and affected all companies (the whole country, even the whole world) at the same time, it provides a unique opportunity to test the protection function of certain factors. In this context, the effects of corporate social responsibility and sustainability factors have received increasing attention. Particularly, the pandemic shifted companies' focus to CSR. CSR has been widely viewed as a protection-like insurance for firms (Flammer, 2013; Godfrey, Merrill, & Hansen, 2009; Krüger, 2015). In such, the stakeholders of more sustainable firms would defend the firms, thus tend to diminish the adverse effect comparing to the worse sustainability performers during a shock. Covid-19 offers an important setting to test whether firms' prior sustainability performance pays off during the crisis.

This study examines the effect of sustainability performance on crisis returns. Specifically, this paper focuses on firms included and excluded in the Istanbul Stock Exchange BIST Sustainability Index. To investigate whether the stock market reaction differs between high- and low-sustainability companies during the outbreak period of the pandemic, the event study methodology is applied. Event study enables to observe how the stock prices reflect to an event by calculating the difference between the realized stock price and the expected stock price. Three critical days – first case, first measures, first death – during

the Covid-19 crisis are considered and investigated. The results show that firms included in the BIST Sustainability Index experience fewer loss comparing to the excluded ones, suggesting that investors value firms' sustainability performance during the crisis outbreak period.

This study contributes to the social responsibility-financial performance literature in terms of investigating whether sustainability plays a protective role in times of crisis, and also contributes to the shareholder behavior area. Besides, this research reveals new findings by using data from the Turkish stock market and enlarge our knowledge related the stock market reactions in developing country studies, which could provide the potential to contribute to overcome generalizability problem. In this sense, the related study offers implications for both theory and practice.

1. Giriş

Korona virüsünün ortaya çıkması ve hızla yayılması sadece toplum üzerinde değil, finansal piyasalarda da şok etkisi yaratmıştır. Bununla birlikte korona virüs salgının etkileri de hızla araştırılmaya başlanmış, ilgili çalışmalar zaman içerisinde derinleşmiş ve artmıştır. Bu kapsamda Covid-19'un özellikle finansal etkileri hem teoride hem de uygulamada üzerinde durulan bir konu olarak karşımıza çıkmaktadır. Salgının finansal etkilerini irdeleyen ilk çalışmalardan biri Zhang, Hu, & Ji (2020) tarafından yapılmış olup bu durumun ülkelerin risk seviyesini arttırdığını ortaya koymuştur. Bunu takip eden Ramelli & Wagner (2020)'in çalışma sonuçları ise uluslararası ticaret hacmi fazla, yüksek borçlu ve az nakdi bulunan firmaların daha düşük kümülatif anormal getiriye sahip olduğunu göstermektedir. Özellikle vakaların tespit edilmesi ve ölümlerin gerçekleşmesine Amerika ve Avrupa borsalarında işlem yapan yatırımcıların negatif tepki gösterdiği söylenebilir (Heyden & Heyden, 2021). Pay piyasalarında oluşan negatif etki Türkiye'de de gözlemlenmiştir (Keleş, 2020; Pakel & Özen; Tan, 2021).

Mevcut çalışmalar olumsuz etkiler konusunda mutabık olmakla birlikte firmaların bu olumsuz etkiden hangi koşullarda daha çok etkilendiği diğer boyutu ile bu tür şoklardan nasıl korunabileceğine ilişkin soruya cevap aramaktadır (Alfaro et al., 2020; Fahlenbrach et al., 2020; Ramelli & Wagner, 2020; Zechner et al., 2020). Korona virüs salgının beklenmedik bir şok olması ve aynı anda tüm firmaları (tüm ülkeyi, hatta tüm dünyayı) etkilemesi nedeniyle belirli faktörlerin koruyuculuğunun test edilmesi bakımından eşsiz bir imkan sağlamaktadır. Bu kapsamda özellikle önemi her geçen gün artan kurumsal sosyal sorumluluk ve sürdürülebilirlik faktörlerinin etkileri merak uyandırmakta olup pandemi ile birlikte firmaların odakları çevresel, sosyal ve yönetim faktörleri merkeze alan sürdürülebilir uygulamalara kaymıştır. Sosyal sorumlu ya da sürdürülebilir kurumsal uygulamalar firmalar için kriz dönemlerinde sigorta benzeri koruyuculuk sağlayabilmektedir (Flammer, 2013; Godfrey et al., 2009; Krüger, 2015). Sürdürülebilirlik performansı yüksek firmaların tüm paydaşları (menfaat sahipleri) ilgili firmalara kriz dönemlerinde bağlı kalıp kötü sürdürülebilirlik performansına sahip firmalara göre krizlerin olumsuz etkilerini azaltmasına

katkı sağlayabilmektedir. Covid-19, firmaların bu tür taahhütlerinin kriz döneminde katkı sağlayıp sağlamadığını araştırmak için önemli bir ortam sunmaktadır.

Bu çalışmada sürdürülebilirlik performansının kriz dönemi pay getirilerine etkileri araştırılmaktadır. Çalışmada BİST Sürdürülebilirlik Endeksi firmalarına odaklanılmaktadır. Pandeminin ülkemizde ortaya çıkma dönemi olarak 1-17 Mart 2020 tarihleri ele alınmış olup, bu dönemde yüksek ve düşük sürdürülebilirlik performansına sahip firmalar arasında pay piyasası tepkisinin farklı olup olmadığını test edilmesi için olay çalışması yönteminden yararlanılmıştır. Olay çalışması bir olay karşısında gerçekleşen ile beklenen getiri arasındaki farkın hesaplanarak pay piyasası tepkisini tespit etmeye yardımcı olmaktadır. Çalışmada Covid-19 krizinin ortaya çıkma dönemi için önemli üç tarih – ilk vaka, ilk kapsamlı sosyal tedbirler ve ilk ölüm – ele alınmış ve incelenmiştir. Çalışma sonuçları BİST Sürdürülebilirlik Endeksinde yer alan firmaların olmayanlara göre daha az etkilendiğini ortaya koymaktadır. Bu da yatırımcıların kurumsal sürdürülebilirlik performanslarını krizin ortaya çıktığı dönemde dikkate aldığını göstermektedir.

Bu çalışma sürdürülebilirliğin kriz anlarında koruyucu bir faktör görevi üstlenip üstlenmemesinin araştırılması bakımından sosyal sorumluluk-finansal performans literatürüne katkı sağladığı gibi, yatırımcı tepkilerinin gözlemlenmesine de katkı sağlamaktadır. Bununla birlikte bu araştırma daha az sayıda olan gelişmekte olan ülke araştırmalarına ülkemiz verileri kullanılarak yeni bulgular ortaya koymaktadır. Çalışmanın böylece genellenebilirlik problemine yönelik de katkı sağlama potansiyeline sahip olduğuna inanılmaktadır. Bu anlamda ilgili çalışma hem teoriye hem de uygulamaya dönük çıkarımlar sunmaktadır.

Çalışmanın devamı ise şu şekildedir: 2. bölümde ilgili literatür verilmektedir. 3. Bölümde veri ve örneklemeden bahsedilerek olay çalışması yöntemine değinilmektedir. Araştırma bulgularının ortaya konduğu 4. bölümden sonra 5. bölümde sonuç ve tartışma yer almaktadır.

2. Literatür

Godfrey (2005), her türlü sosyal sorumluluk faaliyetinin her bir firmanın sosyal ahlaki ser-

mayesini oluşturduğunu ve bu kazanılan sermayenin firmanın kurumsal itibar sermayesine etki ettiğini ifade etmektedir. Firmaların kurumsal itibar sermayesi orta ve uzun vadede firmaların finansal performansını etkilemektedir. Sosyal ahlaki sermaye kurumsal itibar sermayesine katkı sağlayabileceği gibi özellikle firmaların zor zamanlarında (ürün geri çağırma, finansal kriz, skandal gibi) bir koruyucu kalkan oluşturabilir ve firmaların daha az zarar görmesini sağlayabilir (Flammer, 2013; Godfrey et al., 2009; Shiu & Yang, 2017).

Firmaların sosyal sermayelerinin koruyuculuğuna yönelik önemli çalışmalarda sosyal, çevresel ve yönetim (ÇSY) performanslarının firmaların kriz dönemlerini daha az hasarla atlmasına katkı sağlayabildiğine yönelik sonuçlar mevcuttur. 2008-2009 krizinde firmaları koruyup korumadığına ilişkin ilk ve etkili çalışmalardan olan Lins, Servaes ve Tamayo (2017) firma ve paydaşları arasında kurulan güvenin – MSCI ÇSY performans skorları ile ölçtüğü sosyal sermaye ile kurulan – küresel finansal krizde firmaları koruduğunu göstermiştir. Albuquerque vd. (2020) ise Covid-19 krizinin ortaya çıkış dönemi için benzer bir araştırma yapmıştır. Araştırma sonuçları çevre ve sosyal derecelendirme skorları yüksek firmaların düşük olanlara göre 2020'nin ilk çeyreğinde daha iyi performans gösterdiğini ortaya koymaktadır. Bunun yanı sıra farklı sürdürülebilirlik performans göstergeleri de vardır. Bunlar içerisinde sıklıkla kullanılan ve yazında kabul görmüş olan yöntemlerin başında belirli endekslere (örneğin sürdürülebilirlik endeksi, kurumsal yönetim endeksi gibi) dahil olup olmama gelmektedir (Hawn, Chatterji, & Mitchell, 2018; Ramchander, Schwebach, & Staking, 2012).

Finansal piyasalarda firmalar ile yatırımcılar arasındaki bilgi asimetrisi (Greenwald & Stiglitz, 1990) firmaların sürdürülebilirlik uygulamalarının dışardan takibine yönelik ihtiyacı arttırmaktadır. Bu bakımdan Sürdürülebilirlik Endeksi firmaların sürdürülebilirlik performanslarına ilişkin bilgileri ortaya çıkarmaya ve bunu yatırımcılara iletmeyi sağlar (Ramchander et al., 2012). Korona virüs salgınının BIST'e etkileri araştırılmış olmasına karşın (Yılmaz, Aksoy, & Tatoglu, 2020) sürdürülebilirlik performansı yüksek olan veya olmayan firmaların bu krizden nasıl etkilendiklerine ilişkin bir çalışmaya rastlanmamıştır. Yılmaz vd (2020), 2014-2017 yılları arasında Sürdürülebilirlik Endeksine dahil olan firmaların pay getirilerine anlamlı etkisini bulamamış ancak 2016 darbe girişimi sırasında endekse

dahil olmanın piyasalarda koruyucu bir rol oynadığını tespit etmiştir. Bu çalışma ile salgın döneminde sürdürülebilirlik endeksinde yer alan ve almayan firmaların pay piyasalarında oluşan etkilere verdikleri tepkilerin farklılık gösterip göstermediği araştırılmaktadır. Bu amaçla salgının kritik günleri (Keleş 2020) için hesaplanan anormal getirileri sürdürülebilirlik endeksinde olan veya olmayan firmalar için karşılaştırılmıştır. Elde edilen bulgular sürdürülebilirlik endeksinde yer alan firmaların krizin çıkış döneminde daha az olumsuz etkilendiğini ortaya koymaktadır.

3. Veri ve Yöntem

3.1. Veri

Yukarıda bahsedildiği üzere bu çalışma ile sürdürülebilirlik endeksinde dahil olan ve olmayan şirketlerin korona virüs salgınının yarattığı olumsuz finansal etki karşısında göstermiş oldukları tepkiler araştırılmaktadır.

Çalışma örneklemini BIST 30 firmaları oluşturmaktadır. Ülkemizde salgının ortaya çıktığı Mart 2020 döneminden önce yayınlanan Kasım 2019 BIST Sürdürülebilirlik Endeks verileri sürdürülebilirlik performans göstergesi olarak alınmıştır. İlgili yıla ait listede bir sonraki endeks yayınlanma döneminde BIST Sürdürülebilirlik Endeksinde dahil edilecek paylar ile endeksten çıkarılacak paylar sonuçların hatalara sebep olma ihtimali nedeniyle kapsam dışında tutulmuş ve 23 adet endekse dahil olan 5 adet dahil olmayan firma olmak üzere toplam 28 firma örneklemini oluşturmaktadır. BIST 30 endeksinde yer alan şirketler ve BIST Sürdürülebilirlik Endeks bilgileri Tablo 1’de gösterilmiştir.

Tablo 1: BIST 30 Firmaları ve BIST Sürdürülebilirlik Endeks Bilgileri

Sürdürülebilirlik Endeksinde yer alan BİST 30 firmaları	
Akbank Türk A.Ş.	Tofaş-Türk Otomobil Fabrikası A.Ş.
Arçelik A.Ş.	Tüpraş-Türkiye Petrol Rafineleri A.Ş.
Aselsan A.Ş.	Türk Hava Yolları A.O.
Doğan Şirketler Grubu Holding A.Ş.	Türkiye Şişe ve Cam Fabrikaları A.Ş.
Ereğli Demir ve Çelik Fabrikaları T.A.Ş.	Türk Telekomünikasyon A.Ş.
Ford Otomotiv Sanayi A.Ş.	Turkcell İletişim Hizmetleri A.Ş.
Hacı Ömer Sabancı Holding A.Ş.	Türkiye Garanti Bankası A.Ş.
Koç Holding A.Ş.	Türkiye Halk Bankası A.Ş.
Pektim Petrokimya Holding A.Ş.	Türkiye İş Bankası A.Ş.
Soda Sanayii A.Ş.	Türkiye Vakıflar Bankası T.A.O
Tav Havalimanları Holding A.Ş.	Yapı ve Kredi Bankası A.Ş.
Tekfen Holding A.Ş.	
Sürdürülebilirlik Endeksinde yer almayan BİST 30 firmaları	
Bim Birleşik Mağazalar A.Ş.	Koza Altın İşletmeleri A.Ş.
Emlak Konut GYO	Koza Anadolu Metal Madencilik İşletmeleri A.Ş.
Kardemir Karabük Demir Çelik San. ve Tic. A.Ş.	
Sürdürülebilirlik Endeksine bir sonraki dönemde dahil edilecek BİST 30	
Enerjisa Enerji A.Ş.	
Sürdürülebilirlik Endeksinden bir sonraki dönemde çıkarılacak BİST 30 firmaları	
Pegasus Hava Taşımacılığı A.Ş.	

Çalışma kapsamında 1 Mart 2020-17 Mart 2020 dönemi incelenmiştir. Ekonomik tedbir paketinin açıklanmasının yarattığı etkiler ile gözlemlenmesi amaçlanan değişkenlerin örtüşen etkilerden arındırılması için çalışma periyodu ilk ekonomik tedbir paketinin açıklandığı 18 Mart 2020 tarihine kadar ki dönemi ile sınırlandırılmıştır. Bu kapsamda ilk vakanın (10 Mart 2020), ilk tedbirlerin – okulların kapatılması, futbol maçlarının ertelenmesi – (12 Mart 2020) ve ilk ölümün (17 Mart 2020) açıklandığı kritik tarihler çalışma kapsamında incelenmiştir (Keleş, 2020).

3.2. Yöntem

İlgili etkilerin test edilmesi için olay çalışması yönteminden yararlanılmıştır. Bu yöntem Fama (1970)'nin etkin piyasa hipotezine dayanmaktadır. Buna göre bir pay senedinin fiyatı kamuya açık bilgileri anında yansıtmakta, bu da bilgi etkisinin test edilmesine imkân vermekte, ayrıca pay senedinin fiyatını etkileyen faktörleri belirlemeye olanak sağlamaktadır. Anormal getiri, gerçekleşen ile beklenen pay getirileri arasındaki fark olarak hesaplanmaktadır. Bu çalışmada piyasa modeli literatüre dayanarak aşağıdaki gibi tahmin edilmiştir (MacKinlay, 1997)²:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \quad \text{Piyasa Modeli}$$

R_{it} ve R_{mt} sırasıyla i firmasının t günündeki getirisi ile değere göre ağırlıklandırılmış bir piyasa endeksinin t günündeki getirisini göstermektedir. Beklenen pay getirilerini tahmin etmek için 60 geçmiş işlem günü (-70. günden -11. güne kadar) tahmin periyodu olarak kullanılmıştır (Capelle-Blancard & Petit, 2019). α_i ve β_i tahminleri elde edildikten sonra beklenen normal getiriler hesaplanmıştır. En sonunda da olay penceresi boyunca gerçekleşen getiri ile beklenen getiri farkı anormal getiri olarak hesaplanmıştır.

$$AR_{it} = R_{it} - (\hat{\alpha}_i + \hat{\beta}_i R_{mt}) \quad \text{Anormal Getiri}$$

$T_2 < \tau_1 \leq \tau_2 \leq T_2$ eşitliğini sağlayan τ_1 gününden gününe kadar olan Kümülatif Anormal Getiri (KAG; Cumulative Abnormal Return, CAR) aşağıdaki gibi tanımlanmaktadır:

$$CAR_i(\tau_1, \tau_2) = \sum_{t=\tau_1}^{\tau_2} AR_{it} \quad \text{Kümülatif Anormal Getiri}$$

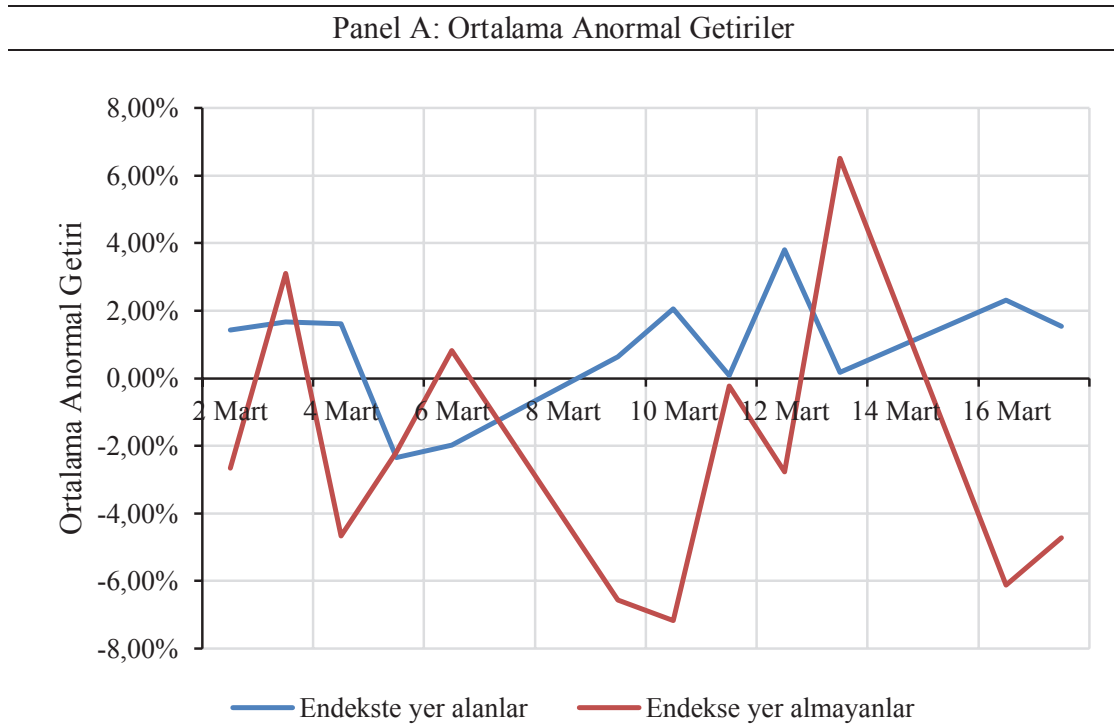
ve τ_1 'den ye kadar olan zaman periyoduna da genellikle is KAG penceresi yada KAG periyodu adı verilmektedir.

² Çalışmada olay çalışması literatürü ile uyumlu olarak gerçekleşen getirileri temsilen logaritmik getiriler kullanılmıştır (i pay senedinin t günü fiyatının doğal logaritması ile $t-1$ günündeki fiyatının doğal logaritması arasındaki fark, $\ln\left(\frac{P_t}{P_{t-1}}\right)$). Bununla birlikte sonuçların dirençliliği için normal getiri (bir önceki güne göre fiyat değişim yüzdesi) ile de benzer sonuç elde edilmiştir.

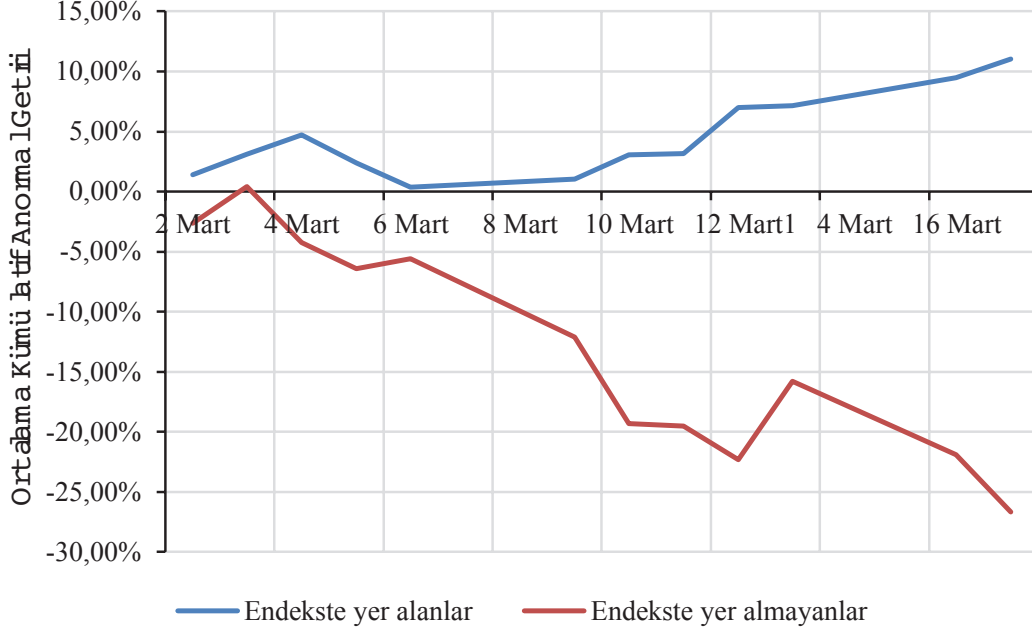
Çalışmada pandeminin ortaya çıkış dönemi için anormal ve kümülatif anormal getiriler hesaplanmıştır. Pencerelemlerin anlamlılığı parametrik ve nonparametrik testler aracılığıyla da test edilmiştir. Parametrik testlerden t-testi, BW t-testleri (Brown & Warner, 1980, 1985) ve Patell z testi (Patell, 1976) istatistikleri; parametrik olmayan testlerden ise Rank z testi (Corrado, 1989) istatistikleri kullanılmıştır.

4. Araştırma Bulguları

Araştırma kapsamında yer alan firmaların 2-17 Mart 2020 tarihleri arasında günlük anormal getirilerinin analizi yapılmıştır. Grafik 1'teki gibi BİST Sürdürülebilirlik Endeksinde yer alan firmalar ile yer almayan firmaların ortalama anormal getirileri ile kümülatif anormal getirileri karşılaştırılmaktadır. Panel A'da günlük ortalama anormal getirilerin endekste yer alan firmalarda yer almayanlara göre daha az oynak olduğu görülmektedir. Örneğin endeks firmaları %-2,18-%3,81 arasında anormal getirilere sahipken, endekste yer almayanların anormal getirilerinin ise %-7,18-%6.51 arasında dalgalandığı tespit edilmiştir. Kısa bir süre dışında genelde bu iki grubun piyasa tepkilerinde farklı davrandığı da dikkat çekmektedir.



Panel B: Ortalama Kümülatif Anormal Getiriler



Grafik 1: Anormal Getiriler

Panel B'de ise bu iki grupta yer alan firmaların Mart ayı başından başlayarak mali tedbir paketine kadar olan süredeki kümülatif anormal getirileri yer almaktadır. Mart başında farklı olsa da paralel olan piyasa tepkisi ikinci hafta ile birlikte ayrılmaya başlamıştır. Özellikle ilk vaka ve ilk ölüm haberleri sonrasında iki grup arasındaki farkın en fazla olduğu görülmektedir. Krizin ülkemizde ortaya çıktığı dönemde endekse dahil olan firmaların ortalama kümülatif anormal getirisi %11,03 iken dahil olmayan grup firmaları için ortalama-%26,65 olarak gerçekleşmiştir. BİST30 firmalarının tamamı için negatif kümülatif anormal getiri (-%4,48) tespit edildiği düşünüldüğünde endeks firmalarının daha iyi performans sergilediği görülmektedir. Bu durum sürdürülebilirlik performansının sonuçlarından biri olan endekste yer almanın krizin ülkemizde ortaya çıktığı dönemde ilgili firmalar için koruyucu rol oynadığı şeklinde yorumlanabilir.

Tablo 2: Sürdürülebilirlik Performansı ve Pay Piyasası Tepkisi

Sürdürülebilirlik Endeksi	OAG	BW 1980	BW 1985	t ist.	Patell z	Rank z
Panel A: İlk Covid-19 vakası – 10.03.2020						
Dahil Olanlar	0,009	2.668***	1.854*	2.097**	3.042***	1.813*
Dahil Olmayanlar	-0,042	-4.894***	-4.018***	-3.364**	-4.661***	-2.529**
Panel B: İlk kapsamlı tedbirler – 12.03.2020						
Dahil Olanlar	-0.007	-1.945*	-1.351	-0.823	-1.568	-0.278
Dahil Olmayanlar	-0.024	-2.767***	-2.272**	-1.269	-2.396**	-1.810*
Panel C: İlk Covid-19 kaynaklı ölüm – 17.03.2020						
Dahil Olanlar	0,000	-0.093	-0.064	-0.037	0.149	0.778
Dahil Olmayanlar	-0.019	-2.224**	-1.826*	-1.44	-1.934*	-1.156

*, ** ve *** istatistiki açıdan sırasıyla %10, %5 ve %1 anlamlılık düzeylerini göstermektedir.

Tablo 2’de ise Covid-19 krizinin ülkemizde ortaya çıktığı dönemin toplum ve piyasalar için bazı önemli tarihlerdeki piyasa tepkisini göstermektedir. Anormal getirilerin anlamlılığını test etmek için de çeşitli test istatistikleri kullanılmıştır. Çalışmada önceki araştırmalarda da kullanılan parametrik ve parametrik olmayan testlerden yararlanılmıştır.

Panel A’daki bulgulara göre sürdürülebilirlik performansı yüksek firmaların ilk vaka açıklaması sonrasında istatistiki olarak % 5 düzeyinde anlamlı hafif pozitif bir tepki (ort. KAG=%0,9, Patell z test ist.=2,097) görülürken, düşük performanslı grup için %1 anlamlılık düzeyinde güçlü negatif tepki (ort. KAG=-%4,2, Patell z test ist.=-4,661). İlk kapsamlı sosyal tedbirlerin alınma duyurusu sonrasında (Panel B) sürdürülebilirlik performansı yüksek firmaların kayıpları sınırlıdır (ort. KAG=%0,7, Patell z test ist.=-1,568, BW1980 test ist.=-1.945).. Buna karşın sürdürülebilirlik performansı düşük grup için %5 düzeyinde anlamlı ve negatif ortalama kümülatif anormal getiriler tespit edilmiştir (ort. KAG=-%2,4, Patell z test ist.= -2.396). Panel C ise Covid-19 pandemisinde ülkemizdeki ilk resmi ölüm haberi sonrasında yatırımcıların tepkisini göstermektedir. Bu tarihteki tepkiler de önceki iki tarihle benzerdir. Sürdürülebilirlik endeks firmaları belirgin bir kayıp yaşamaz-

ken, düşük performanslı diğer firmaların kümülatif anormal getirileri negatif ve istatistiki olarak %10 düzeyinde anlamlıdır (ort. KAG=-%1.9, Patell z test ist.=-1.934).

Özetle, Covid-19 pandemisinin ülkemizdeki ilk döneminde sürdürülebilirlik performansı yüksek firma paylarının kriz dönemi getirilerinin daha yüksek olduğu görülmektedir. Bu bulgular, (i) firmaların sosyal sermaye yatırımlarının kriz döneminde yatırımcıların bu firmalara diğerlerine göre daha fazla güven duymasına yol açtığı (Lins et al., 2017) ve sigorta benzeri bir koruyuculuk sağladığı (Godfrey et al., 2009); (ii) yatırımcıların sosyal sorumlu uygulamalara sahip ve sürdürülebilirlik performansı yüksek olan firmalara karşı yüksek sadakatli olduğu ve bunun arttığına (Albuquerque et al., 2020; Heinkel, Kraus, & Zechner, 2001; Pástor & Vorsatz, 2020) yönelik görüşler ile de uyumludur.

Sonuç

Tüm dünyada olduğu gibi ülkemizde de Covid-19 pandemisi finansal piyasalarda inanılmaz fiyat ve işlem hacmi değişimlerine neden olmuştur. Bu çalışmada ile Covid-19 pandemisinin ortaya çıkış döneminde firmaların pandemi öncesindeki sürdürülebilirlik performanslarının koruyuculuğu araştırılmıştır. Buna göre yatırımcılar ilk vaka, ilk tedbir ve ilk ölüm haberlerine sürdürülebilirlik performansı yüksek firmalar için daha ılımlı tepki vermiştir. Pandemi öncesinde sosyal sermayesi güçlü olmayan firmalar ise krizin bu döneminde daha fazla olumsuz etkilenmişlerdir. Bu sonuçlar aynı zamanda sürdürülebilirliğin sosyal sermaye oluşumuna yol açtığı ve bunun krizlerde sigorta benzeri koruyuculuk sağladığı görüşleriyle uyumludur.

Bu çalışma sürdürülebilirliğin kriz anlarında koruyucu bir faktör görevi üstlenip üstlenmesinin araştırılması bakımından sosyal sorumluluk-finansal performans literatürüne katkı sağladığı gibi, yatırımcı tepkilerinin gözlemlenmesine de katkı sağlamaktadır. Bununla birlikte bu araştırma daha az sayıda olan gelişmekte olan ülke araştırmalarına ülkemiz verileri kullanılarak yeni bulgular ortaya koymaktadır. Çalışmanın böylece genellebilirlik problemine yönelik de katkı sağlama potansiyeline sahip olduğuna inanılmaktadır. Bu anlamda ilgili çalışma hem teoriye hem de uygulamaya dönük çıkarımlar sunmaktadır.

Çalışma örnekleme pandeminin çıkış dönemi ve BİST30 firmaları (Sürdürülebilirlik endeksine dahil olan ve olmayan) ile sınırlıdır. Bu nedenle sonraki dönemler ve BİST 30 kapsamı dışındaki firmaların dahil edilmesi gibi boyutlarıyla çalışma genişletilebilir.

Çıkar Çatışması

Yazar herhangi bir çıkar çatışması olmadığını beyan eder.

Finansal Destek

Yazar bu çalışma için herhangi bir finansal destek almamıştır.

Hakem Değerlendirmesi

Dış Bağımsız

Kaynakça

Albuquerque, R., Koskinen, Y., Yang, S., & Zhang, C. (2020). Resiliency of Environmental and Social Stocks: An Analysis of the Exogenous COVID-19 Market Crash. *The Review of Corporate Finance Studies*, 9(3), 593–621. <https://doi.org/10.1093/rcfs/cfaa011>

Alfaro, L., Chari, A., Greenland, A. N., & Schott, P. K. (2020). Aggregate and firm-level stock returns during pandemics, in real time. National Bureau of Economic Research.

Brown, S. J., & Warner, J. B. (1980). Measuring security price performance. *Journal of Financial Economics*, 8(3), 205–258. [https://doi.org/https://doi.org/10.1016/0304-405X\(80\)90002-1](https://doi.org/https://doi.org/10.1016/0304-405X(80)90002-1)

Brown, S. J., & Warner, J. B. (1985). Using daily stock returns: The case of event studies. *Journal of Financial Economics*, 14(1), 3–31. [https://doi.org/https://doi.org/10.1016/0304-405X\(85\)90042-X](https://doi.org/https://doi.org/10.1016/0304-405X(85)90042-X)

Capelle-Blancard, G., & Petit, A. (2019). Every Little Helps? ESG News and Stock Market Reaction. *Journal of Business Ethics*, 157(2), 543–565. <https://doi.org/10.1007/s10551-017-3667-3>

Corrado, C. J. (1989). A nonparametric test for abnormal security-price performance in event studies. *Journal of Financial Economics*, 23(2), 385–395. [https://doi.org/https://doi.org/10.1016/0304-405X\(89\)90064-0](https://doi.org/https://doi.org/10.1016/0304-405X(89)90064-0)

Ding, W., Levine, R., Lin, C., & Xie, W. (2020). Corporate immunity to the COVID-19 pandemic. National Bureau of Economic Research.

Fahlenbrach, R., Rageth, K., & Stulz, R. M. (2020). How valuable is financial flexibility when revenue stops? Evidence from the COVID-19 crisis. National Bureau of Economic Research.

Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance*, 25(2), 383–417. <https://doi.org/https://doi.org/10.1111/j.1540-6261.1970.tb00518.x>

Flammer, C. (2013). Corporate Social Responsibility and Shareholder Reaction: The Environmental Awareness of Investors. *Academy of Management Journal*, 56(3), 758–781. <https://doi.org/10.5465/amj.2011.0744>

Godfrey, P. C. (2005). The Relationship Between Corporate Philanthropy And Shareholder Wealth:

A Risk Management Perspective. *Academy of Management Review*, 30(4), 777–798. <https://doi.org/10.5465/amr.2005.18378878>

Godfrey, P. C., Merrill, C. B., & Hansen, J. M. (2009). The relationship between corporate social responsibility and shareholder value: an empirical test of the risk management hypothesis. *Strategic Management Journal*, 30(4), 425–445. <https://doi.org/https://doi.org/10.1002/smj.750>

Greenwald, B. C., & Stiglitz, J. E. (1990). Asymmetric information and the new theory of the firm: Financial constraints and risk behavior. National Bureau of Economic Research.

Hawn, O., Chatterji, A. K., & Mitchell, W. (2018). Do investors actually value sustainability? New evidence from investor reactions to the Dow Jones Sustainability Index (DJSI). *Strategic Management Journal*, 39(4), 949–976. <https://doi.org/https://doi.org/10.1002/smj.2752>

Heinkel, R., Kraus, A., & Zechner, J. (2001). The Effect of Green Investment on Corporate Behavior. *The Journal of Financial and Quantitative Analysis*, 36(4), 431–449. <https://doi.org/10.2307/2676219>

Heyden, K. J., & Heyden, T. (2021). Market reactions to the arrival and containment of COVID-19: An event study. *Finance Research Letters*, 38, 101745. <https://doi.org/https://doi.org/10.1016/j.frl.2020.101745>

Keleş, E. (2020). COVID-19 ve BİST-30 Endeksi Üzerine Kısa Dönemli Etkileri. *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 42(1), 91–105.

Krüger, P. (2015). Corporate goodness and shareholder wealth. *Journal of Financial Economics*, 115(2), 304–329. <https://doi.org/https://doi.org/10.1016/j.jfineco.2014.09.008>

Lins, K. V., Servaes, H., & Tamayo, A. (2017). Social Capital, Trust, and Firm Performance: The Value of Corporate Social Responsibility during the Financial Crisis. *Journal of Finance*, 72(4). <https://doi.org/10.1111/jofi.12505>

MacKinlay, A. C. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, 35(1), 13–39.

Pakel, C., & Özen, K. (2020). Daily Volatility Analysis of BIST 100 Constituents Between 2018-2020. *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 42(2), 340–360.

Pástor, L., & Vorsatz, M. B. (2020). Mutual fund performance and flows during the COVID-19 crisis. *The Review of Asset Pricing Studies*, 10(4), 791–833.

Patell, J. M. (1976). Corporate Forecasts of Earnings Per Share and Stock Price Behavior: Empirical Test. *Journal of Accounting Research*, 14(2), 246–276. <https://doi.org/10.2307/2490543>

Ramchander, S., Schwebach, R. G., & Staking, K. I. M. (2012). The informational relevance of corporate social responsibility: evidence from DS400 index reconstitutions. *Strategic Management Journal*, 33(3), 303–314. <https://doi.org/https://doi.org/10.1002/smj.952>

Ramelli, S., & Wagner, A. F. (2020). Feverish Stock Price Reactions to COVID-19*. *The Review of Corporate Finance Studies*, 9(3), 622–655. <https://doi.org/10.1093/rcfs/cfaa012>

Shiu, Y.-M., & Yang, S.-L. (2017). Does engagement in corporate social responsibility provide strategic insurance-like effects? *Strategic Management Journal*, 38(2), 455–470. <https://doi.org/https://doi.org/10.1002/smj.2494>

Tan, Ö. F. (2021). The Impact of News about Pandemic on Borsa Istanbul during the COVID-19 Financial Turmoil. *Türkiye İletişim Araştırmaları Dergisi*, (37), 1.

Yilmaz, M. K., Aksoy, M., & Tatoglu, E. (2020). Does the Stock Market Value Inclusion in a Sustainability Index? Evidence from Borsa Istanbul. *Sustainability*, Vol. 12. <https://doi.org/10.3390/su12020483>

Zechner, J., Pagano, M., & Wagner, C. (2020). Disaster resilience and asset prices.

Zhang, D., Hu, M., & Ji, Q. (2020). Financial markets under the global pandemic of COVID-19. *Finance Research Letters*, 36, 101528. <https://doi.org/https://doi.org/10.1016/j.frl.2020.101528>

Özgeçmiş

Emrah KELEŞ, Marmara Üniversitesi İşletme Fakültesinde Dr. Öğretim Üyesi olarak görev yapmaktadır. Marmara Üniversitesinde Muhasebe-Finans Doktorasını almıştır. Varlık fiyatlama, medya, kurumsal sosyal sorumluluk ve davranışsal finans gibi konularda araştırmalar yapmaktadır.

Research Article/ Araştırma Makalesi

THE EXTERNAL FINANCIAL STATEMENT AUDIT PROCESS AND BLOCKCHAIN TECHNOLOGY

Graham GAL¹

Matthew SHERWOOD²

Submitted/Başvuru: 15.06.2021

Last Revised/Son Düzeltme: 29.07.2021

Accepted/Kabul: 30.07.2021

Abstract

This study examines the relationship between the financial statement audit process and blockchains. While clients' use of blockchain technology might provide some benefits to external auditors' substantive testing procedures, those benefits appear very limited, and an increase in controls testing effort is likely to offset any reduction in substantive audit effort. This is due to blockchain technology's inability to provide assurance regarding most of the financial statement assertions external auditors test. The study notes that many of the purported benefits of blockchain technology to the auditing profession, such as the ability to test a full set of transactions and the potential for real-time auditing, existed before the development of blockchain. Thus, while blockchain is likely to have some effect on the auditing profession, it is hard to say to what extent that impact might be.

Keywords: Blockchains, Independent Audit, Internal Controls

JEL Classification: M15, M42, 033

1 Associate Professor Dr., Department of Accounting, Isenberg School of Management, University of Massachusetts, Amherst, MA 01003 USA
gfgal@isenberg.umass.edu, ORCID ID:0000-0001-6526-9367

2 Assistant Professor Dr., Department of Accounting Isenberg School of Management, University of Massachusetts, Amherst, MA 01003 USA
msherwood@isenberg.umass.edu, ORCID ID:0000-0001-5856-5003

To cite this article: Gal, G., & Sherwood, M. (2021). The External Financial Statement Audit Process and Blockchain Technology. *TİDE Academia Research*, 3(1), 105-142

Öz

Bu çalışma finansal tabloların denetim prosedürü ile blokzincirler arasındaki ilişkiyi incelemektedir. Müşterilerin blokzincir teknolojileri dış denetçilerin maddi doğruluk testi yöntemlerine bazı faydalar sağlayabilirken bu faydalar çok sınırlı kalabilir ve iç kontrol testlerindeki artışla maddi doğruluk denetimlerindeki azalış dengelenebilir. Bunun sebebi, blokzincir teknolojisinin dış denetçilerin test ettiği mali tablo iddialarının çoğuna ilişkin güvence sağlayamamasıdır. Bu çalışma blok zinciri teknolojisinin denetim mesleğine sağladığı söylenen, tam bir işlem setini test etme yeteneği ve gerçek zamanlı denetim potansiyelinin bulunması gibi bazı faydalarının çoğunun blok zincirinin geliştirilmesinden önce de var olduğuna dikkat çekiyor. Bu bağlamda, blokzincirin denetim mesleği üzerinde bir miktar etkisinin olması ihtimal dahilinde olsa da bu etkinin ne ölçüde olabileceğini söylemek zor.

Anahtar kelimeler: Blokzincirler, Bağımsız Denetim, İç Kontroller

JEL Sınıflandırması: M15, M42, 033

1. Introduction

Advancements in technology have led to fundamental changes in the way businesses process their transactions, and report results. For instance, developments in computing hardware and software allow firms to capture and process increasingly large sets of transaction-level data, in relatively less time. While this makes it easier for management access and analyze the firm's transactions, the lack of a tangible record of each transaction makes its validation more difficult. Despite this challenge, the likelihood of organizations reverting to the use of more hard copy transactions is remote, which in turn makes the data quality assurance of firms' transactions, and subsequent performance disclosures, increasingly important and challenging. Obtaining an external financial statement audit, is one-way firms attempt to provide outsiders with assurance regarding the validity of their disclosed transactions. At the same time auditors also face challenges stemming from changes in technology. Auditors have to adjust their processes to account for the fact that clients' information can be captured and stored in multiple settings and locations, exist in multiple computer systems, be processed by software created by different vendors, and can be accessed by multiple users at multiple locations (Rittenberg & Schwieger, 2001). Further, to continue to be able to provide relevant assurance services, auditors need to adapt to how technology alters the way their clients conduct and record their business activities.

In addition to general complexity increases in clients' information systems, the audit process has been affected by regulatory change and advances in auditor-developed technologies. Section 404(b) of the Sarbanes Oxley Act requires financial statement auditors to assess their clients' internal control procedures, which are to create, process, allow access, and generally influence the quality of the data used in financial disclosures (United States Congress, 2002).³ While audits always included some review of internal controls, Sarbanes-Oxley mandates auditor review and opine on the Internal Controls over Financial Reporting (ICFR) of their external audit clients. In 2002, the SEC issued rule changes to accelerate the filing of quarterly and annual reports, which resulted in an acceleration of the audit completion date. Auditors, in part, used new technologies to cope with the

³ This increased recognition of the importance of reviewing financial reporting processes has also been shown in the review of cybersecurity (Steinbart, Raschke, Gal, & Dilla, 2016; 2018)

reduced audit timeline. These included advances in electronic working paper software, automating roll forward and leads sheet generation, expanded use of Computer Assisted Auditing Techniques (CAATs) and development of Continuous Controls Monitoring (CCM) systems.⁴ Certainly, these technologies have significantly increased the reliability of the audit process (Rittenberg & Schwieger, 2001). However, auditors still face concerns about reviewing the quality of the increasingly large and complex sets of transaction-related data clients use to produce financial statements and disclosures. While clients' adoptions of some recent technologies, such as cloud computing, seem to make data quality assessment harder for the external auditor, enterprise blockchain platforms are being perceived by some as a solution to auditors' data quality assessment issues within financial reporting procedures.

Enterprise blockchain platform (EBP) technology has several unique qualities, some of which might be able to address certain data quality concerns companies face with regards to their financial reporting procedures. For instance, once a block of transactional data is added to the blockchain, users with access to the blockchain, can readily identify any alterations to its block's contents. The locking of data within a chain of blocks often referred to as an "immutable ledger," is a core aspect of all blockchain technologies, and ensures no subsequent changes to details including the transaction's values and date. While some of the properties of blockchains provide some assurance on certain measures of data quality there are other assertions made by management concerning their financial statements that could also be impacted by the use of blockchains. Thus, accounting and reporting concerns, such as ensuring the accuracy of a product's historical purchase price, or the period in which a transaction occurs, become known with certainty. The idea, that recording transactions using an EBP can result in an immutable ledger, has led to claims that inherent accounting assurances blockchain offers, will end the need for other external assurance mechanisms, such as independent financial statement audits. Certainly, features such as those described above and in the subsequent section, make EBP technology amenable to address specific accounting and reporting risks. However, are they a panacea that will solve

⁴ While the suggestion to use software to continuously review transactions, or add in audit work is not new (Vasarhelyi & Halper, 1991) the use of CAATs and CCM within the external audit setting has become more prevalent (Kogan, Alles, Vasarhelyi, & Wu, 2014).

all accounting and reporting related assurance concerns and remove the need for external assurance of the financial statements? If not, what financial reporting procedures and external audit areas, might an EBP affect or not affect? The purpose of this manuscript is to address the changes that might ensue to the financial reporting process and to the auditing of financial statements as a result of the adoption of EBP. Specifically, the paper will discuss the potential effects of EBP adoption on the quality of companies' transactional data, and accounting processes and how this might affect external auditors' procedures, and testing, with regards to their assessments of management's assertions over their financial statements.

The remainder of this paper is organized as follows. Section 2 looks at blockchains in more detail and discusses the characteristics, which could impact companies' data quality, accounting procedures, and financial statement preparation. Section 3 highlights the financial reporting process, describes management's assertions over the firm's financial statements, and briefly discusses typical external financial statement audit procedures. Section 4 presents a set of comprehensive examples that examine how adopting a distributed transaction repository EBP or a smart contract EBP might affect data quality and accounting procedures, as well as how each might affect how auditors validate managements' assertions. Section 5 discusses how EBPs might influence public accounting firms, and Section 6 presents a summary, conclusions, and implications.

2. Blockchain Technology

As the name implies, a blockchain is a series of information "blocks" that are connected. The chaining of the blocks creates a time sequence in which order is preserved in such a way as to make reordering of events difficult if not impossible. The core components of each block are a set of transactions sent by participants to the chain during a short period of time. While other types of transactions, such as smart contracts, are being considered for blockchains, at this time exchanges of cryptocurrencies predominate on blockchains.

Participants on the blockchain are assigned a key or wallet. Much like a traditional bank account, the wallet contains an amount of cryptocurrency exchanged on the particular blockchain. The wallet has a public key which is used to locate the wallet on the chain, and

a private key which is the owner's link to the wallet. Depending on the type of blockchain the owner of the wallet may be anonymous.⁵ Each participant can add or accept transactions sent to the chain, and after a transaction is included in a block each participant will get an updated copy of the entire set of blocks. For a transaction to be added to a block, it must be verified, and accepted by a simple majority (51%) of the chain's participants.⁶ There are a couple of steps in the verification process, and the finalization of an exchange transaction. First, the user digitally signs the transaction, indicating the recipient's wallet id, includes an amount of coin that is to be exchanged on the particular chain, and an amount of the coin to run the transaction.⁷ Different chains exchange different types of coin. It is envisaged that it would be easy to have exchange transactions across multiple chains, and therefore transactions which have multiple types of coins or resources. To accomplish these multiple resource exchanges, a number of issues need to be addressed (Back, et al., 2014). Wang & Kogan (2018) provide an example of the interaction of sidechains where different types of coins, representing different assets, are exchanged. The Accounting Blockchain Coalition (ABC) has also looked at different types of digital assets, including asset tokens which embody a claim against the issuer, utility tokens which allow the wallet holding them to access an application or service, payment tokens can be used to acquire goods or services, and hybrid tokens which have some characteristics of the others. These classifications are critical as different jurisdictions consider certain types of digital assets as securities while others do not (Accounting Blockchain Coalition Internal Controls Working Group, 2019). For example, the International Monetary Fund faces the problem of determining which digital assets, particularly if it is issued by a country, should be viewed as financial reserves (He, 2018). As a second step in the verification process, the exchange transaction is timestamped. This timestamping preserves the order of transactions. While timestamping of transaction is necessary to prevent double-spending, it is not sufficient. One potential threat to double spending is in fast payment implementations (Karame, Androulaki, Roeschlin, Gervais, & Capkun, 2012). Because final

5 In permissionless blockchains the owners of wallets are usually anonymous while in permissioned blockchains the parties are usually known to other participants (Vukolić, 2017). However, even in permissioned blockchains there are techniques which can be used to reduce anonymity (Meiklejohn, et al., 2016; Ron & Shamir, 2013).

6 A blockchain is made up of nodes each of which contain a complete set of blocks. This ensures that no one node can alter either the order of the blocks or the information on transactions without the knowledge of all other participants.

7 On the Ethereum blockchain the payment to run the transaction is called "gas".

verification occurs when the exchange transaction is added to a block on the blockchain, and this may not occur for a few minutes, it is possible to use a coin in two fast payment transactions, where multiple exchanges occur in that time frame; such as for a cup of coffee (Karame, Androulaki, & Capkun, 2012). Another potential threat to double spending attacks occurs when there is a fork in the blockchain; an alternative chain is introduced at a particular block (Wirachantika, Barmawi, & Wahyudi, 2019). While, not quite the same as a traditional double spending attack, a user can alter the order of exchanges as they appear on the blockchain, by attaching a higher processing fee to a transaction. This fee provides a financial incentive to the miners which will finalize the inclusion of a transaction in a block. Therefore, by attaching a higher fee to one transaction an owner of a wallet can cause one transaction to appear to have occurred prior to what was actually an earlier transaction. Because of scalability issues with bitcoin type blockchains, the delay in propagation of transactions to the other participants, can allow modification of the information (Gervais, Ritzdorf, Karame, & Capkun, 2015).

The process of creating an immutable block of transactions is done through “mining”. Mining is the process of accepting a set of transaction into a block, and propagating this new block to all chain participants. The key to the immutability of both the blocks in the chain and to the information contained in each block is a set of hashes. Hashing algorithms are mathematical functions which take a string as input and produce a digital representation (Ali Orumiehchiha, Pieprzyk, & Steinfeld, 2012; Bellaire, Jaeger, & Len, 2017; Hamer, 2002; National Institute of Standards and Technology, 2015). There are many classifications of these algorithms, but they have two essential attributes (Chi & Zhu, 2017). First, the digital representation, the hash, should change if there are any changes to the input string. Second, there should be few if any collisions. The first attribute implies that a hash can provide evidence that a set of information, the string, has been altered. However, to actually find any change depends on the length of the string; a change in a six-word sentence would be easier to find than a change in a 6 trillion record database. The hash of a set of transactions in a block should detect a change in any of the characters which make up the contents of the block. The second attribute is a measure of the probability that two different strings will yield the same hash; their hashes collide. This attribute is similar to the first but has a slightly different implication. The first implies a quick test to see if a set

of information, a string of any length, has changed. The second determines how easy it is to change the string and keep the same hash. Regardless of the hashing algorithm there is a non-zero probability of a collision; two different strings yield the same hash. For blockchain implementations, changing the original transaction's wallets to a different receiving or sending wallet that is sending the cryptocurrency would be a significant change. The probability of finding the exact alteration that could make such a change undetectable used to be quite remote. However, with the advent of quantum computers this is no longer a remote possibility (Bryanov, 2019).

For the bitcoin blockchain, the hash for a block is based on the content of the transactions included in the block, the date, and a number called a nonce (Cryptoticker, 2019). The transactions to be included in the block are hashed in a hierarchical tree structure called a Merkle Tree (Merkle, 1980; USA Patent No. US4309569, 1982). The top node of the tree contains a hash of the top branches, these branches contain the hash of the branches at the next level, and so on with the hash of individual transactions at the lowest level. The hash for a block on the bitcoin chain must meet certain structural constraints. Through the process of "mining" the hash of the Merkle Tree, and the other information in the block is converted into the block's hash. Each blockchain can choose a particular algorithm to arrive at a consensus on way in which this mining is to take place (Chi & Zhu, 2017; Tan, Hu, & Wang, 2019). In the bitcoin blockchain the information in each transaction (and so the hash at the top of the Merkle Tree) and the date are fixed, so to meet the constraints on the address or hash of the block the miner iterates through possible values for the nonce until a solution is reached. The miner that solves the problem of identifying a hash which satisfies bitcoin's Proof-of-Work (PoW) consensus requirement receives a set number of bitcoins in payment. It is estimated that in 2018 miners were required to iterate through 25.0 million tera hashes per second to solve bitcoin's PoW.⁸ The required computing power to find a nonce has resulted in pools of miners that collaborate on the work provided (Sheehan, et al., 2017).

These requirements, to have an encrypted wallet, to create a hash of the information in

⁸ A tera hash is 1x10¹² hashes. Thus, to compete for bitcoin's mining prize requires the computing ability to iterate through 25x10¹² hashes per second (Yang, 2018).

the block, and the mining supports a level of assurance on the integrity of the information in a specific block. The creation of links to previous blocks preserves the temporal order of blocks. So, the hashing of information in a block, and the linking of the blocks in a chain preserves both some level of assurance on the integrity and the potential to ascertain when transactions occurred. However, it is not necessary that the information on the blockchain is correct. First, even if a wallet sends an exchange transaction to the chain it is not verified immediately, and so there is a period of time between sending and confirming the exchange. This period may not be critical unless there is some need to use the results of an exchange in a subsequent exchange – the oil was received and the gas was produced and subsequently delivered. While some have argued that a ledger on the blockchain can include the accounting for both sides of the transaction (Dai & Vasarhelyi, 2017), there are some difficulties with this approach. The blockchain is a set of transactions in “Collaboration Space” (International Organization for Standardization and the International Electrotechnical Commission, 2007). The blockchain works because no single party determines what a particular exchange means; one party's cash receipt is another party's cash disbursement. In more complex transactions, forcing the blockchain to one party's view of the transaction, limits its applicability; one party's raw material is another party's finished good. In addition, if the exchange is for a particular cryptocurrency, it is difficult to determine whether the other side of the exchange has taken place. For instance, if an amount of cryptocurrency is sent to a wallet with the expectation of delivery of some other asset, such as inventory, the actual delivery is off-chain.⁹ Therefore, for complete information in a supply chain it would be necessary to include access to off chain sensors (Hussain, 2017). To support audit of information on the blockchain, another issue that must be considered is the precise timing of the exchange.

The time used for blockchain exchanges is UnixEpoch time (Epoch Converter, 2019). This is based on seconds from a specified time (January 1, 1970 00:00:00) at Coordinated Universal Time.¹⁰ As exchanges are mined into a block, the time of the block will be different than the time the transaction was executed and may also be different than the

9 It has been suggested that the Internet of Things (IoT) can bring movement of all assets to the blockchain (Christidis & Devetsikiotis, 2016; Dai & Vasarhelyi, 2017). This move of transactions to “collaboration space” requires a different type of contract and a view of contracted resources as types and delivery as instances (McCarthy, Geerts, & Gal, 2021)

10 In some countries this is referred to as Greenwich Mean Time.

time it was sent to the block. This difference could be small; however, there is a potential issue with the time. As blockchains deal with exchanges on a global scale the block's times can change some recognition issues. The time assigned to an exchange could differ from the time at the actual location of the exchange. This difference could potentially differ by a day, two minutes before midnight versus one minute after midnight, which could make a payment late according to the terms of a contract. Additionally, an exchange could also be mined in a different year which would change amounts in a firm's financial statement.

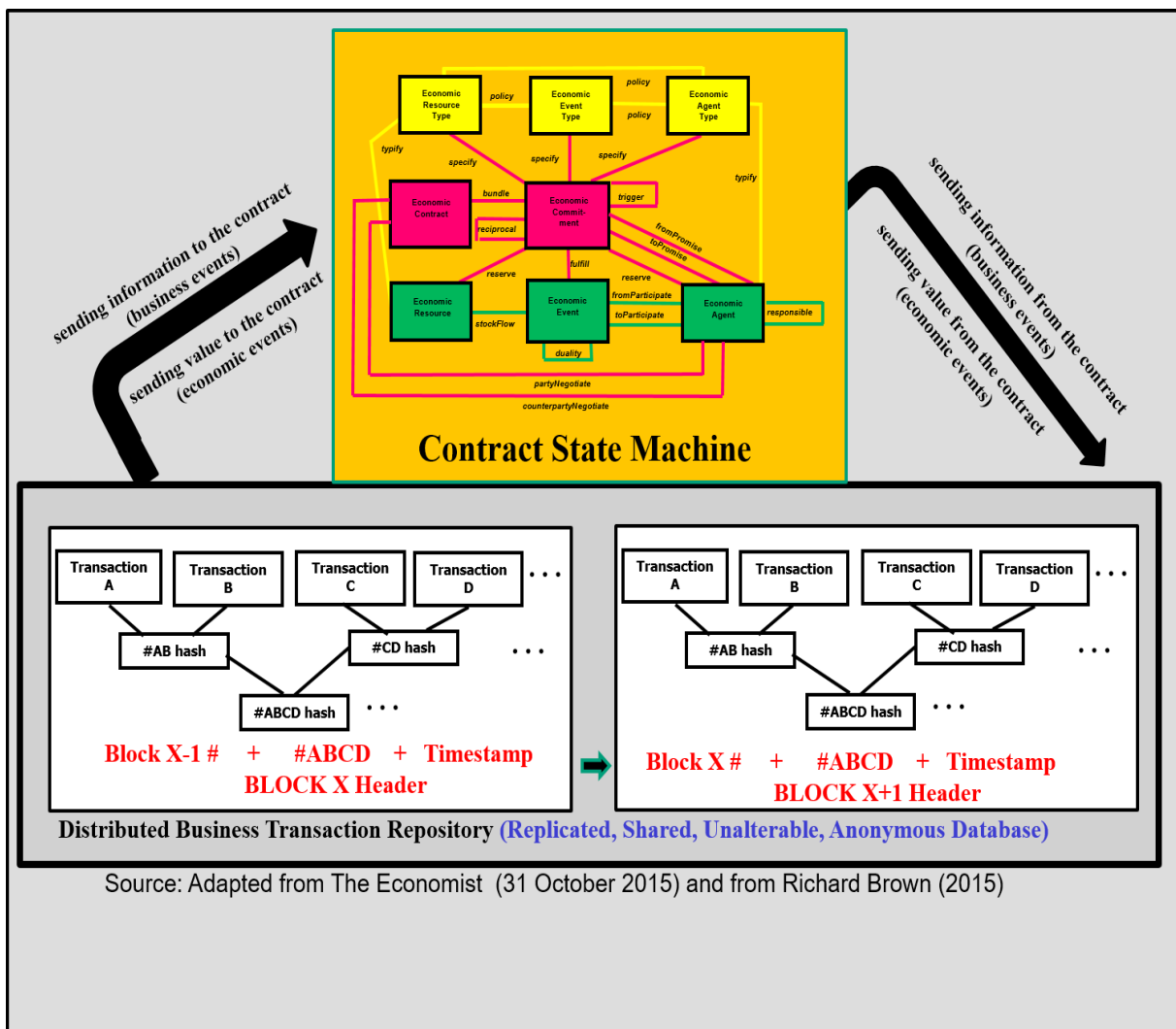


Figure 1 A Distributed Business Transaction Repository State Machine

(Source The REA Ontology, McCarthy, Geerts, and Gal 2021)

While smart contracts (Luu, Chu, Olickel, Saxena, & Hobor, 2016) are not currently a pervasive part of blockchains they certainly are part of its future. A smart contract is computer code containing statements which look for actions which meet conditions of an agreed upon exchange. The processes which complete these actions are off chain and in most cases are the result of firm's business processes.¹¹ Figure 1 depicts the relationship between a firm's information system and blockchains. Figure 1 shows a representation of the REA classes and associations (McCarthy, Geerts, & Gal, 2021) that are related to data in the chain's blocks. When smart contracts are designed, there is a relationship to states in the firm's information system. The economic events are those that are mined into the blocks while contracts are based on type images and indicate a control structure within the firm. For instance, before authorizing transfer a cryptocurrency payment, the state "received merchandise" must occur. Therefore, the firm's information system must recognize the state, and send a message to the smart contract that the state has been completed. So, controls in the organization must include both a determination of state changes, and authorization for the transfer messaging. The mechanics of state machines can enforce the requisite controls over the states in the organization to execute a smart contract (Haugen, 2002; Horiuchi & McCarthy, 2011; Horiuchi & Shimizu, 2016). However, other organizational controls are necessary to ensure the proper execution of the business events which result in the addition of exchanges to the blockchain (Accounting Blockchain Coalition Internal Controls Working Group, 2019).

This section has examined some of the features of blockchains that can ensure the integrity of the information; once mined into the blockchain it cannot be easily changed. However, blockchains cannot provide complete assurance of the veracity of the data; information on the chain indicates that inventory was delivered, but this does not mean that inventory was of the correct quantity and quality. Therefore, an audit over the financial information contained in the chain is necessary to provide reasonable assurance of the financial statements. The next section examines the audit process as it relates to the blockchain.

11 There are some events which become part of smart contract conditions, such as a date at which payment must be received or the contract becomes void.

3. The Financial Reporting Process and Blockchain

3.1 Financial Statement Preparation

The previous section presented some of the important issues that must be considered when a company uses blockchains to perform exchanges of resources. While blockchains can ensure that the data has not been altered, it cannot ensure that the data matches the information concerning the exchange of resources not actually contained in the chain. This section looks at financial reporting and audits of this information when blockchains keep some of the company's information.

Figure 2 presents a high-level overview of the general financial reporting process that firms use to generate the financial statements regulators, investors, and other outside stakeholders require. In the most basic of terms, the financial reporting process consists of three steps. First, the firm engages in and records business transactions. The firm groups and summarizes like-kind business transactions, netting the inflows and outflows within balances against one another. Finally, assigning the net transaction amounts to financial statement lines. To allow for comparability of financial statements among firms, financial statement line items are consolidated and presented based on regulatory guidelines.¹² Firms then close their books for the period, and the process begins anew.

12 In the United States the financial reporting guidelines are established by the Financial Accounting Standards Board. Financial reporting in other countries is regulated by the International Accounting Standards Board.

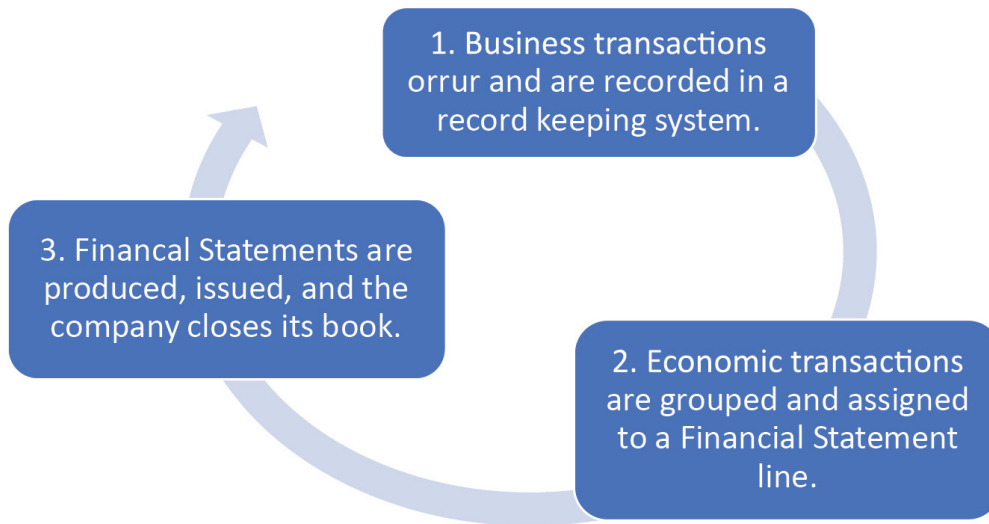


Figure 2 The Financial Reporting Process

The Financial Reporting Process	
1.	Business transactions occur during the firm’s normal course operations. They include things such as acquiring raw materials, producing a service or product, making sales, paying employees, and paying taxes, just to name a few. Companies typically record transactions in their order of occurrence (i.e., chronologically) in their company database. Economic transactions are then recorded as journal entries. Each entry debits at least one account and credits at least one account. The journal entries are transferred from their cycle-specific sub-ledgers to the general ledger. The journal entries are sorted based on the account receiving the debt or the credit.
2.	The general ledger accounts are summed to produce a listing of each account’s balance, known as the trial balance. The firm records any necessary adjusting entries, which are summed with the trial balance, to create an adjusted trial balance. The adjusted trial balance accounts are assigned to a financial statement line item based on the firm’s chart of accounts.
3.	The financial statement produced and made available to management and to shareholders. The company then closes its books for the fiscal year and begins the process anew in the subsequent fiscal year.

A nuanced description of the financial reporting process is beyond the scope of this manuscript. However, a few specific details about the typical financial reporting process will aid our subsequent discussion. First, firms can, and do, use a variety of technologies, ranging from simple spreadsheets to complex Enterprise Resource Planning systems (ERP), to record business transactions. Second, when business transactions are captured they are assigned a unique identifier – a primary key, and then when they are converted to accounting records they are assigned a unique journal entry number. The journal entry number is essential as it allows users of the accounting system (e.g., firm employees and the external auditors), to identify the specific components of each economic transaction or event. Many aspects of an external financial statement audit rely on transaction-level data. However, while regulators govern the presentation of financial statements and disclosures, there are no regulations on internal record-keeping methodologies. Thus, there is no basis for comparison of data across companies at the transaction-level.

Blockchain technologies seem the most poised to impact the creation and recording of transactions steps in the financial reporting process that. As discussed in the prior section, blockchain technology is conceptually broad, and its role still somewhat undefined. However, there are currently two technologies within the enterprise blockchain space that are at the forefront; smart contracts, and distributed transaction repositories.¹³ While both use the same basic blockchain concepts, and there is some overlap between them, their primary focuses differ. A detailed discussion of similarities and differences of these technologies, as well as the companies, platforms, features, and programming languages used to develop specific blockchain technologies, is beyond the scope of this paper.¹⁴ However, it is necessary to touch upon both of these technologies as their role within the financial statement audit process will be examined in the following section of this paper.

One of the many players in the smart contract space is Ethereum, which is an open-source distributed public blockchain network.¹⁵ It allows for the building of decentralized appli-

13 Blockchains have sometimes been referred to as distributed transaction repository, however, a better term is the distributed transaction repository as this indicates a record of transactions as opposed to a record of accounting entries (International Organization for Standardization and the International Electrotechnical Commission, 2019)

14 For more information on these topics as well as academic articles regarding these topics please see: Dai, J., & Vasarhelyi, M. A. (2017).

15 Other smart contract firms include EOS, Cardano, and RSK..

cations (DAPP), which can incorporate smart contract functionality. One such example of a smart contract DAPP built on Ethereum is Quorum, which was developed by J.P. Morgan. Quorum allows for high speed and high throughput processing of private transactions among a group of known, and allowed participants; this is an example of a permissioned blockchain. A noted advantage of Quorum is the use of partial state databases, which creates a network that is partly public and partly private. When the conditions trigger the execution of a contract, the transaction recorded within the blockchain will be hashed and available to anyone with permission to view the block. However, the specific details of the transactions will be encrypted and visible only to users who receive a decryption key from the transaction manager.

In the distributed transaction repository space several companies are working with the Linux Foundation's opensource Hyperledger project.¹⁶ Hyperledger is neither a tool nor a platform like Ethereum, but rather an umbrella strategy with multiple platforms for developing enterprise solutions. Whereas the focus of smart contracts, at least for the moment, is primarily on financial and insurance industries, Hyperledger's focus is on allowing firms to personalize blockchains to address the specific needs of their firm. Hyperledger blockchains are private and permissioned networks that can allow for smart contract transactions (known as chain code) to occur. Channels within Hyperledge, provide a private subnet of communication and allow transactions between premised members, that are accessible only to permissioned network members.

The ultimate role that blockchain technology might play in the financial reporting process is still unknown. However, based on the current iteration of the technology, it appears that the most significant role is likely to be on recording and storing transactions. At its core, the current blockchain technology is a shared data warehouse, the contents of which are verifiable by any member with access to the chain. The fact that multiple members of a chain have a copy of the transactional history makes it difficult, if not impossible, for firms or individuals to change or alter past transactions without the other members of the chain knowing. Distributed transaction repositories' potential to generate immutable records of

¹⁶ Key member firms of Hyperledge include IBM, SAP, Intel, Oracle, and Microsoft. For a full list of Hyperledge members see <https://www.hyperledger.org/members>.

transactions will create a single shared record of transactions. Under traditional systems both parties would create a record of an exchange transaction, but under a distributed transaction repository only one record is needed. Therefore, each party has a record of the transaction that can be used in the production of their financial statements. Smart contracts can reduce human intervention in the recognition of the terms of exchanges. Together these technologies will likely influence not only the production of financial statements, but also the process of providing financial statement assurance.

4. Independent Financial Statements Assurance

4.1. Financial Statement Audit Process

The term audit refers to inspection or examination performed by someone other than the preparer or performer. More specific to this setting Rittenberg and Schweiger's (2001, p. 13), definition of an audit as a, "...systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events ..." Accounting standards, such as US GAAP and IFRS, represent the established criteria to which auditors are to compare the financial statements. While the framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013), provides the criteria for testing the internal controls over financial reporting (ICFR).

The external auditor is typically engaged to assess three aspects of the auditee's financial reporting process. First, did the auditee follow the accounting standards when recording their business activities? Subsequent to the passage of the Sarbanes-Oxley legislation (United States Congress, 2002) a second assessment includes an evaluation of the effectiveness of ICFR. Third, are the amounts reported within the auditee's financial statements materially correct? During an audit, the external audit team performs procedures to obtain evidence allowing them to form an opinion on the reasonableness of the auditee's claim that the financial statements are materially accurate and ICFR are effective.¹⁷ The auditor then issues a report expressing their opinion on the financial statements and effectiveness of the ICFR. Figure 3 presents a summarized overview of the financial statement auditing process.

17 While their discussion in detail is beyond the scope of this paper, two keys aspects of a financial statement audit are independence, and materiality. Generally, independence in this setting means, not both not having a financial interest in an audit client, as well as maintaining an appearance of independence from the client's management. Materiality refers to the fact that auditors are to provide "reasonable" not "absolute" assurance regarding the accuracy of the financial statements.

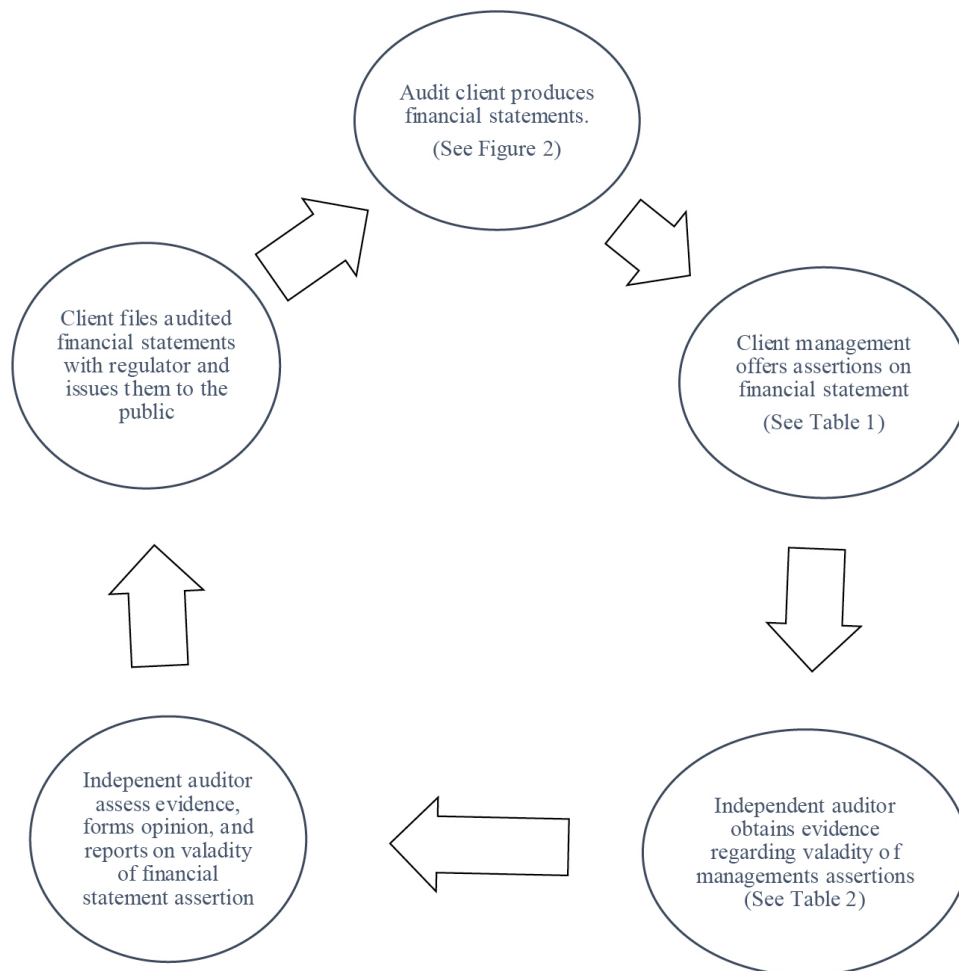


Figure 3 Life Cycle of a Financial Statement Audit

Note: The above diagram outlines the general lifecycle of the annual financial statement audit. The process begins with the client engaging in and recording business activities. The business activities are summarized to form the client's financial statements. The client makes assertions about the financial statements, and the external auditor performs audit tests to obtain evidence regarding the validity of those assertions. Based on the results of the audit tests, the external auditor forms an opinion about the degree to which the financial statements conform to reporting standards (e.g., U.S. GAAP, IFRS, or any local standards) and issue an audit report presenting the auditor's opinion. The client includes the auditor's report when filing their financial statements with the appropriate regulatory body.

The use of blockchains can impact this process in a few ways. First, some of the events which are related to the financial statements may now be executed by smart contracts. Thus, the code actually plays a role in recording of economic transactions. This means that the auditor must have a way to inspect the smart contract's code, to have assurance that the terms of the contract are appropriate, and then perform relevant tests to verify the contract executes (and creates the requisite transactions) as designed. As some of the firm's assets are contained in a blockchain wallet, the auditor must confirm that controls over the access to the wallet are sufficient (Accounting Blockchain Coalition Internal Controls Working Group, 2019).

4.2 Management Assertions

When a company issues financial statements, its management explicitly or implicitly makes assertions (i.e., claims) regarding the financial statement's adherence to accounting standards, the operating effectiveness of the ICFR, and the accuracy of the values reported. It is the auditor's job to perform procedures so they can assess the validity of management's assertions. In many ways, management's assertions are technology agnostic, as it does not matter if the firm records its transactions using paper and pencil, a spreadsheet, or an ERP. Regardless of the mechanism by which firms store their transactional data, they must process and present the data following reporting criteria. While a client's choice in technology might influence the tools an auditor uses to assess the validity of management's assertions, the technology cannot replace the need to perform the procedures. Table 1, presents management's assertions as defined by both the PCAOB and the AICPA.¹⁸

¹⁸ As this manuscript focuses on the external financial statement audits required by the SEC for publicly traded firms our discussion centers on the PCAOB's defined management assertions. However, due to the significant similarities between PCABO and AICPA assertions, the conclusion drawn can be applied to both sets of assertions.

Table 1 Management's Financial Statement Assertions

Panel A: PCAOB Financial Statement Assertions - per Auditing Standard 1105.11

- *Existence or occurrence*—Assets or liabilities of the company exist at a given date, and recorded transactions have occurred during a given period.
- *Completeness*—All transactions and accounts that should be presented in the financial statements are so included.
- *Valuation or allocation*—Asset, liability, equity, revenue, and expense components have been included in the financial statements at appropriate amounts.
- *Rights and obligations*—The company, holds or controls rights to the assets, and liabilities are obligations of the company at a given date.
- *Presentation and disclosure*—The components of the financial statements are properly classified, described, and disclosed.

Panel B: AICPA Financial Statement Assertions - per AU §326.15

Note: This table presents management's assertions regarding the company's financial statements as defined by the PCAOB and the AICPA. Please see <https://pcaobus.org/Standards/Auditing/Pages/default.aspx> and <https://www.aicpa.org/research/standards/auditattest/sas.html>, for the complete set of PCAOB and AICPA auditing standards, respectively.

Certainly, the state of enterprise blockchain technology within the financial reporting and financial statement auditing arenas is not very mature. Firms can choose among the various enterprise blockchain technologies to pursue, and to what degree they want to incorporate that technology into their financial reporting process. Different levels of implementation and adoption of differing blockchain technologies will impact the way in which transaction data is capture and maintained by the firm's information system. However, as noted above, smart contracts and distributed transaction repositories are currently at the forefront of enterprise blockchain solutions. Within the realm of those two block-

chain technologies, the aspects of the financial reporting process whose change is likely to be affected the most are the quality and storage of clients' data and the clients' accounting processes. Despite the level of implementation of these technologies, auditors still have a set of evidence gathering procedures as outlined in Table 2. These procedures are technology independent and therefore it is critical to consider how blockchains might impact evidence gathering. As a result, in the following pages, we provide a set of comprehensive examples that examine the potential impact on the external audit of changes to clients' data quality and accounting procedures in relation to clients' adopting distributed transaction repositories, or smart contract blockchain technologies.

Table 2 Audit Evidence Gathering Procedures per PCAOB AS 1105

AS 1105 paragraph	E v i d e n c e Type	Description
.15	<i>Inspection</i>	<p>Inspection involves examining records or documents, whether internal or external, in paper form, electronic form, or other media, or physically examining an asset. Inspection of records and documents provides audit evidence of varying degrees of reliability, depending on their nature and source and, in the case of internal records and documents, on the effectiveness of the controls over their production. An example of inspection used as a test of controls is inspecting records for evidence of authorization.</p>
.16	<i>Observation</i>	<p>Observation consists of looking at a process or procedure being performed by others, e.g., the auditor’s observation of inventory counting by the company’s personnel or the performance of control activities. Observation can provide audit evidence about the performance of a process or procedure, but the evidence is limited to the point in time at which the observation takes place and also is limited by the fact that the act of being observed may affect how the process or procedure is performed.</p>

.17	<i>Inquiry</i>	Inquiry consists of seeking information from knowledgeable persons in financial or nonfinancial roles within the company or outside the company. Inquiry may be performed throughout the audit in addition to other audit procedures. Inquiries may range from formal written inquiries to informal oral inquiries. Evaluating responses to inquiries is an integral part of the inquiry process. Note: Inquiry of company personnel, by itself, does not provide sufficient audit evidence to reduce audit risk to an appropriately low level for a relevant assertion or to support a conclusion about the effectiveness of a control.
.18	<i>Confirmation</i>	A confirmation response represents a particular form of audit evidence obtained by the auditor from a third party in accordance with PCAOB standards.
.19	<i>Recalculation</i>	Recalculation consists of checking the mathematical accuracy of documents or records. Recalculation may be performed manually or electronically.
.21	<i>Analytical Procedures</i>	Analytical procedures consist of evaluations of financial information made by a study of plausible relationships among both financial and nonfinancial data. Analytical procedures also encompass the investigation of significant differences from expected amounts.

Note: The table describes specific audit procedures per AS 1105 of the PCAOB's auditing standards. The purpose of an audit procedure can be a risk assessment procedure, a test of controls, or a substantive procedure.

third column outlines why the enterprise blockchain technology (a distributed transaction repository in Table 3, a smart contract in Table 4) might provide validity to the financial statement assertion(s). The fourth column outlines why the enterprise blockchain technology (a distributed transaction repository in Table 3, a smart contract in Table 4), might not provide validity to the financial statement assertion(s). The final column presents what, if anything, the procedure from Table 2 auditor might consider doing to gain sufficient validation of management's particular financial statement assertion(s).

For the sake of simplicity, we provide a short description of the assertion here. However, we refrain from reporting the fictitious financial statement values, or how blockchain technology might or might not validate the assertion, as well as from describing what additional procedures the auditor might perform, as that information is contained below within Tables 3 and 4.

As shown in the first column, the first set of assertions shown in each panel of Tables 3 and 4 is that of existence or occurrence. The existence assertion, is primarily applicable to balance sheet line items, and relates to whether the assets or liabilities claimed by the company, via its financial statements, exist as of the financial statement date. Occurrence is the counter-part of existence and deals with the validity that the recorded transactions included in the financial statements, truly represent the events that occurred during a given period and is primarily applicable to the income statement. For exchanges captured in DTR the information about the exchange is immutable, it cannot be changed, and therefore there is a high level of assurance in the occurrence of the transaction. For transactions coded in smart contracts, there is also a high level of assurance on the existence of exchanges. Thus, both block chain technologies provide a high level of assurance on the existence or occurrence assertion.

The second row of the first column of both panels of Tables 3 and 4 contains the completeness management assertion. The completeness assertion addresses whether all of the transactions that should be included and represented within the financial statements are, and that only the transactions which should be include have been. Both technologies, distributed transaction repository and smart contracts, provide assurance for this asser-

tion. However, the auditor would need to verify the controls over DTR while with smart contracts the auditor would need to reconcile the transaction activity.

The third row of the first column of both panels of Tables 3 and 4 contains the rights and obligations financial statement assertion within our example. This assertion indicates that the company holds or controls the rights to the assets and is responsible for the liabilities and other obligations, as indicated on the financial statement, as of the financial statement date. With each of these technologies the information is cannot be changed without a significant effort, which probably cannot occur in a timely fashion. Therefore, each of the technologies provides a high level of assurance that this assertion is supported.

The fourth row of the first column of both panels of Tables 3 and 4 contains the management assertions of valuation or allocation. This assertion relates to whether the financial statements report asset, liability, equity, revenue, and expense components at their appropriate amounts. This might include the recording of valuation adjustments to present assets at their fair or net realizable values. This assertion is problematic for each of the technologies. In each case there are actions which are outside of the blockchain that have a significant impact on valuation. For example, if a transaction represents an exchange with an outside supplier for inventory, with the result in a payable, the auditor must still perform additional procedures to verify that the inventory was received and that it has the appropriate value. This implies that blockchain technologies do not replace the need to observe physical inventories.

The fifth and final row of the first column of both panels of Tables 3 and 4 contains the management assertion of presentation and disclosure. As the term suggests, this assertion relates to whether the components of the financial statements are correctly classified, described, and disclosed. It also includes making sure that the financial statements include all of the required disclosures and the accompanying footnotes. Unfortunately, neither of the blockchain technologies can be relied upon for proper presentation. An auditor must rely on other controls to ensure that information is presented correctly.

Table 3 Panel A
 Fun Toys, Inc. Example
 Enterprise Blockchain Technology Type: Distributed transaction repository Financial
 Reporting Process: *Data Quality*

<p>Assertion</p>	<p>Fun Toys, Inc.</p> <p>The financial statements (F/S) of Fun Toys indicate an inventory balance of \$5.42 million, and costs of sales of \$27.1 million.</p>	<p>How might an Enterprise Blockchain Distributed transaction repository validate the assertion?</p> <p>The use of a Distributed transaction repository Enterprise Blockchain Platform (DTR-EBP), allows both Fun Toys and their business partners to record the shared activity once. This results in a verifiable, third-party record the auditor might rely upon regarding the occurrence of transactions. Presuming that Fun Toys would not pay for items not received, the ledger also verifies that at one point, the inventory purchased did exist.</p>	<p>How might a Distributed transaction repository not validate the assertion?</p> <p>While the use of a DTR-EBP can provide assurance around transaction occurrence, it cannot assure that assets physically exist as of the F/S date. Thus, despite the DTR-EBP indicating the acquisition of real assets (e.g., inventory), it does not provide validation that those assets continue to exist. Also, the DTR-EBP can only provide assurance regarding the transaction recorded using it. Any activity that Fun Toys records outside of the DTR-EBP will receive no assurance.</p>	<p>What additional procedures might the auditor consider?</p> <p>The auditor will need to perform audit procedures (e.g., physical inspection) to ensure the assets, which Fun Toys claims are real, and still in their position, are, in fact, real and still in their position. The auditor will also need to perform audit procedures on any activity that Fun Toys records outside of the DTR-EBP.</p>
<p>Completeness</p>	<p>The F/S of Fun Toys indicate a cash and equivalents balance of \$5.97 million and an advertising expense of \$5.24 million.</p>	<p>If Fun Toys records all of their activity using a DTR-EBP, the auditor can verify each transaction and the date of its occurrence. If the auditor can reconcile the net transaction activity per Fun Toys DTR-EBP with the balances per the F/S, the auditor can determine if only the transactions, as well as all of the transactions occurring within the fiscal period, are reported, in the F/S.</p>	<p>Even if the transactions per the DTR-EBP are reconciled to the F/S, the auditor will need to determine if all of the transactions that should be reflected in the F/S are. Otherwise, the auditor runs the risk of Fun Toys engaging in activity outside of the DTR-EBP and failing to consolidate it with the activity per the DTR-EBP.</p>	<p>The use of a DTR-EBP allows for a reduction in human intervention. However, the auditors will need to reconcile the balances per the DTR-EBP with the F/S and perform audit procedures on reconciling items. The auditor will also need to test for transactions that should be included in the F/S but are not.</p>

Table 3 Panel A Continued

<i>Assertion</i>	<i>Fun Toys, Inc.</i>	<i>How might an Enterprise Blockchain Distributed transaction repository validate the assertion?</i>	<i>How might a Distributed transaction repository not validate the assertion?</i>	<i>What additional procedures might the auditor consider?</i>
Rights and Obligations	The F/S of Fun Toys, indicate the company's accounts receivable balance is \$9.7 million and accounting payable balance is \$4.22 million.	Fun Toys can track their exchanges of goods using a DTR-EBP. Given the distributed nature, both Fun Toys and their business partners record the transaction separately, resulting in a verifiable, third-party record, the auditor might rely upon regarding the rights of ownership and obligation, as the parties provide validation of the transactions with one another. Fun Toys can be either a buyer or seller, depending on the transaction. Thus, if all of Fun Toys purchases or sales occur via a DTR-EBP the auditor can verify, summarize, and compare all of the DTR_EBP balances, to the balances per the F/S.	Fun Toys will not be able to conduct all of its sales and purchases via a DTR-EBP. As a result, Fun Toys will need to maintain a separate set of records to account for sales and purchases occurring outside the DTR-EBP, which it will need to summarize and use it to reconcile the DTR-EBP balances with the F/S. Obviously, the DTR_EBP will not provide the auditor assurance with regards to the transactions recorded outside of the DTR-EBP.	The auditor will need to obtain details of the transactions occurring outside of the DTR-EBP and will need to perform sufficient audit procedures and gather evidence, as to the rights and obligations pertaining to this activity. The auditor will also need to reconcile the combined DTR-EBP and non-DTR-EBP activity with the F/S and perform audit procedures over the reconciling activity.

Table 3 Panel A Continued

<p>Valuation or Allocation</p>	<p>The F/S of Fun Toys, indicate the company's accounts receivable balance is \$9.7 million and accounting payable balance is \$4.22 million.</p>	<p>Similar to the rights and obligation assertion, if a DTR-EPB is used, then the known transaction values can be obtained via the multi-party immutable ledgers, which can lend validity to the amounts per the F/S.</p>	<p>Similar to rights and obligations, it is unlikely all transactions will occur via a DTR-EBP. Unlikely rights and obligations, valuation and allocation, include significant management estimates, of items such as the allowance for doubtful accounts, and fixed asset depreciation. It is unclear how management would record estimates via a DTR-EBP. Further, as these entries only affect Fun Toys there will be no third-parties to validate the DTR-EBP.</p>	<p>As Fun Toys is the only affected party, it is unlikely that the adjusting transactions would be recorded using a DTR-EBP. Thus, to test these assertions, the auditor will need to perform significant procedures to determine if management's assumptions are reasonable. The auditor will also need to perform audit procedures around any transactions recorded outside of the DTR-EBP.</p>
<p>Presentation and Disclosure</p>	<p>Management asserts the F/S and disclosures comply with US-GAAP.</p>	<p>The use of a DTR-EBP might allow the auditor to confirm the accuracy of the values within the F/S.</p>	<p>The use of a DTR-EBP will not provide any comfort on if the F/S comply with US-GAAP.</p>	<p>The auditor will need to review the F/S and test any deviations between reporting requirements and how the F/S are presented.</p>

Panel B

Enterprise Blockchain Technology Type: Distributed transaction repository

The aspect of the Financial Reporting Process: Accounting Procedures

<i>Assertion</i>	<i>How an Enterprise Blockchain Distributed transaction repository might not validate the assertion?</i>	<i>What additional procedures might the auditor consider?</i>
Existence or Occurrence	Despite Fun Toys' ability to auto-order and make and receive payments via a DTR-EBP, their auditor will still need to perform validation testing to ensure that the items Fun Toys paid for were the actual items that were received. Further, the auditor will need to review the relevant policies to understand and test which transactions should be occurring within the DTR-EBP.	After understanding which transactions, the DTR-EBP should be processing, the auditor needs to test both the DTR-EPB controls and its activity. The controls testing is to ensure that authorized activity is occurring. The activity testing is to assess if accounting policies are being followed.
Completeness	While the use of a DTR-EBP might be able to ensure that all of the transactions within the DTR-EBP are represented in the F/S, it cannot ensure that Fun Toys has engaged in all required transactions. Thus, the auditor will need to ensure that any required transactions have taken place within the proper period.	The auditor of Fun Toys will need to review and be familiar with all relevant accounting and regulatory policies. The auditor will then need to review the transactions of Fun Toys either within or outside of the DTR-EBP to ensure that all necessary transactions, have occurred.

Table 3 Panel B Continued

<i>Assertion</i>		<i>What additional procedures might the auditor consider?</i>
Rights and Obligations		The auditor will need to test the details of all transactions occurring outside the DTR-EBP to ensure they are accurately reflected within the F/S. The auditor will also need to test if the DTR-EBP activity is in accordance with Fun Toys accounting policies
Valuation or Allocation		The auditor will need to gain a detailed understanding of key valuation policies (e.g., allowance for bad debts, fixed asset depreciation). The auditor will need to test the activity around these items, to ensure accounting policies are being followed.
Presentation and Disclosure		The auditor will need to test the F/S to ensure reporting requirements are being followed.

Table 4 Panel A
 Enterprise Blockchain Technology Type: *Smart Contracts*
 Mass-York Bank Corp. *Example*

<i>Assertion</i>	<i>Mass-York Bank Corp.</i>	<i>How an Enterprise Blockchain Smart Contract might validate the assertion?</i>	<i>How an Enterprise Blockchain Smart Contract might not validate the assertion?</i>	<i>What additional procedures might the auditor consider?</i>
Existence or Occurrence	The Mass-York financial statements (F/S) claim that as of the end of the fiscal year, the institution has cash holdings of \$573 million and engaged in hedge position swaps resulting in revenue of \$181 million.	The use of a decentralized application (DAPP) built on an enterprise blockchain platform (EBP) will allow the auditor to track and confirm the value of transactions conducted with a third party also using the DAPP. This will create an immutable ledger based on these transactions and will provide the auditor comfort over the occurrences of the transactions, and the existence of account balances equal to the transactions net ending balance.	The auditors will only be able to obtain comfort on these assertions with regards to the transactions, and the net ending account balances, that are recorded using the smart contract EBP.	At a minimum, the auditor will need to reconcile the transaction activity and the net ending balances per the EBP and the F/S to ensure that the balances and activity per the F/S agree to the activity recorded via the EBP. The auditor will need to thoroughly investigate and test any differences between the F/S and the EBP, as well as activity occurring outside of the EBP.
Completeness	The Mass-York F/S indicate general operating expenses of \$3.24 million.	If Mass-York records all transactional activity using a smart contract EBP, the auditor can use the beginning account balances, the net activity, and the ending accounting balances to verify that all expected transactions have been recorded.	Even if the auditor is able to confirm that all the transactions recorded in the F/S should have been, EBP is unable to provide validation to the auditor that all transactions which should have been recorded within the EBP, actually were recorded.	The auditor will need to test any activity recorded outside of the EBP. Further, the auditor will need to perform audit procedures to look for and examine any activity that should have been included within the F/S and was not.

Table 4 Panel A Continued

<i>Assertion</i>	<i>Mass-York Bank</i>	<i>How an Enterprise Blockchain Smart Contract might validate the assertion?</i>	<i>How an Enterprise Blockchain Smart Contract might not validate the assertion?</i>	<i>What additional procedures might the auditor consider?</i>
Rights and Obligations	The F/S of Mass-York indicate the company's mortgage receivable balance is \$179 million, and the long-term debt payable balance of \$526 million.	Mass-York can track their exchanges of goods using an EBP. Given DAPP's nature, both parties in the transaction, can record the transaction separately, which can lend validity to rights of ownership after the exchange. Mass-York can be either the buyer or seller. Thus, if all of Mass-York's activities occur via EBP, the auditor could verify Mass-York's EBP activity, summarize it, and reconcile it to the F/S.	It is unlikely that Mass-York will have the ability to conduct all of its activity via a smart contract EBP. As a result, Mass-York will need to maintain a separate set of records that account for the activity that occurs outside of the EBP. Obviously, the EBP will not be able to provide any support to the validity of the transactions or net account balances of the activity recorded outside of the EBP.	The auditor will need to obtain the details of all activity that occurs outside of the EBP. The auditor will need to reconcile the balances and activity per the EBP with the F/S, using the activity recorded outside of the system. The auditor will then need to perform sufficient audit procedures to gather evidence as to the rights and obligations pertaining to the reconciling activity.
Valuation or Allocation	The F/S of Mass-York indicate the company's mortgage receivable balance is \$179 million, and the long-term debt payable balance of \$526 million.	Similar to the rights and obligation assertion, if Mass-York uses a smart contract EBP, then the known transaction values can be obtained, and the immutable ledgers can lend validity to the amounts per the F/S.	It is unlikely all activity will occur via a EBP. Thus, activity outside of the EBP will not be validated by a trading partner. Additionally, valuation and allocation include management estimates, for items such as the realizable value. It is unclear to what extent management would record estimates via an EBP, as estimates are internal operational decisions.	The auditor will need to obtain the summarized EBP values and reconcile them to the F/S. These reconciling items are likely to include both activities occurring outside of the EBP and internal estimates. The auditor will then need to test the assertions on the activity and internal estimates.
Presentation and Disclosure	Management asserts the F/S and disclosures comply with US-GAAP.	The use of an EBP might allow the auditor to confirm the accuracy of the values within the F/S.	The use of an EBP will not provide comfort as to if the F/S presentation and disclosures comply with US-GAAP.	The auditor will need to test the F/S to ensure reporting requirements are being followed.

Panel B
Enterprise Blockchain Technology Type: *Smart Contracts*
The aspect of the Financial Reporting Process: *Accounting Procedures*

<i>Assertion</i>	<i>Mass-York Bank Corp.</i>	<i>How an Enterprise Blockchain Smart Contract might validate the assertion?</i>	<i>How an Enterprise Blockchain Smart Contract might not validate the assertion?</i>	<i>What additional procedures might the auditor consider?</i>
Existence or Occurrence	The financial statements (F/S) of Mass-York claim that as of the end of the fiscal year, the institution has cash holdings of \$573 million and engaged in hedge position swaps resulting in revenue of \$181 million.	The use of a decentralized application (DAPP) built on an enterprise blockchain platform (EBP) will allow the auditor to investigate the consistency with which the transactions conducted with a third party are recorded. The immutable ledger based on the multi-party transactions and will provide the auditor comfort that transaction did occur and are not fictitious entries.	The auditor will only be able to obtain comfort with the validity of these assertions with regards to the transactions, and the net ending account balances, that are recorded using the smart contract EBP. For example, if the accounting policy calls for an activity to occur automatically when a condition is met, the smart contract EBP does not provide evidence that a sale occurred every time that the condition is met.	At a minimum, the auditor will need to reconcile each EBP with the appropriate Mass-York accounting policy. The auditor will need to review and then investigate, any differences between the operation of the EBP and company policy.
Completeness	The Mass-York F/S indicate general operating expenses of \$3.24 million.	If Mass-York records all transactional activity using a smart contract EBP, the auditor will be able to validate the volume and dates of occurrence of the transactions.	While the smart contract EBP will provide details such as the date of the transactional activity, it will not provide evidence with regards to if the smart contracts execute transactions in-line with the associated accounting policies or regulatory guidance.	At a minimum, the auditor will need to reconcile each EBP with the appropriate Mass-York accounting policy. The auditor will also need to ensure that any changes made to the EBP are done so in a time manner to ensure all transactions are occur in line with company expectations.

Table 4 Panel B Continued

<i>Assertion</i>	<i>Mass-York Bank Corp.</i>	<i>How an Enterprise Blockchain Smart Contract might validate the assertion?</i>	<i>How an Enterprise Blockchain Smart Contract might not validate the assertion?</i>	<i>What additional procedures might the auditor consider?</i>
Rights and Obligations	The F/S of Mass-York indicate the company's mortgage receivable balance is \$179 million, and the long-term debt payable balance of \$526 million.	If Mass-York tracks their exchanges of goods using smart contracts within an EBP, the auditor will be able to validate the ownership rights and performance obligations of the transactions recorded via the smart contract EBP.	While the smart contract EBP will provide details of the transactions recorded within it, the EBP will not provide evidence with regards to if the firm continues to retain the rights and the obligations that have been recorded within the smart contract EBP.	The auditor will need to reconcile each EBP with the appropriate Mass-York accounting policy. The auditor will want to ensure that the smart contracts are performing as expected, and in accordance with Mass-York's policies. The auditor will also need to test the design of new or revised EBPs.
Valuation or Allocation	The F/S of Mass-York indicate the company's mortgage receivable balance is \$179 million, and the long-term debt payable balance of \$526 million.	The use of a smart contract EBP by Mass-York will provide validation of the historical costs of their transactions. The fact that the other party within each transaction has agreed to the terms of the transaction and recorded them via the immutable ledger, validates the value of the transactions.	Simply because the other party agrees with the price or allows the transaction to occur does not ensure that the internal policies of Mass-York are being followed. As a result, the auditor will be unable to determine if internal policies are being followed, as well as if Mass-York is complying with regulatory policies.	At a minimum, the auditor will need to reconcile each EBP's with the appropriate Mass-York accounting policy. The auditor will need to test if the smart contracts follow Mass-York's accounting policies. The auditor will need to thoroughly review and test any differences between how the EBP is operating, and the accounting policies.
Presentation and Disclosure	Management asserts that the presentation of the F/S and disclosures comply with US-GAAP.	The use of an EBP might allow the auditor to confirm the accuracy of the values within the F/S.	The use of an EBP will not provide comfort as to if the F/S presentation and disclosures comply with US-GAAP.	The auditor will need to test the F/S to ensure reporting requirements are being followed.

6. Conclusion

Since its introduction in 2008, the concept of blockchain technology has undergone rapid advances. This has led to an expansion of the technology from the world of crypto-currencies into mainstream applications, such as smart contracts and distributed transaction repositories. While the processing of data via blockchain technology is typically automated, the quality and accuracy of the recorded transactions remain limited to the accuracy and correctness of the transaction parameters established within the blockchain source code. The use of blockchain technology might reduce the potential for error due to human intervention during the processing phase of the accounting cycle. However, this reduction in risk will be offset by an increase in the risk of error within the transaction processing source code of any blockchain tool.

The identification of this transfer of risk is important, as it highlights the continued necessity for external assurance of firms' financial reports even within the realm of blockchain-based accounting systems. While the recording of activity via a blockchain might occur outside the control of the management, the ability to provide accurate and reliable data to external stakeholders is reliant on the processes and procedures put in place by management. Thus, while the adoption of blockchain might alter the manner in which an independent accountant obtains assurance over a client's financial statements, it does not reduce or remove the need of an external assurance provider.

By using both a distributed transaction repository and smart control example, this manuscript presents the potential relation between blockchain technology and the external audit process. In particular, it examines the following three questions. How might an Enterprise Blockchain Distributed transaction repository validate the assertion? How might a Distributed transaction repository not validate the assertion? What additional procedures might the auditor consider? This manuscript presents the relationship between management assertion concerning information contained in financial statements and the implications that the use of blockchains have on these assertions. This manuscript differs from studies on the effects of blockchain on accounting and auditing as it does not co-mingle blockchain with other emerging technologies, nor does it present a prototype of how the technology might be applied within a new accounting ecosystem. Rather

this manuscript strips away other new technologies to focus solely on the potential relation between blockchain technologies and the external audit of the financial statements by an independent accountant.

Author Contribution

The authors have equal contribution to the paper.

Conflict of Interest

There is no conflict of interest among the authors.

Financial Support

The authors have not received any financial support for this study.

Peer-Review

Externally peer-reviewed

References

Accounting Blockchain Coalition Internal Controls Working Group. (2019). Digital token classification and definitions. New York: Accounting Blockchain Coalition.

Accounting Blockchain Coalition Internal Controls Working Group. (2019). Possible threats and vulnerabilities of assets related to digital assets and blockchain transactions and possible internal control activities and actions to address them. New York: Accounting Blockchain Coalition.

Ali Orumiehchiha, M., Pieprzyk, J., & Steinfeld, R. (2012). Cryptanalysis of RC4-Based hash function. Proceedings of the Tenth Australasian Information Security Conference (pp. 33-38). Melbourne, VIC: Association for Computing Machinery.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Wuille, P. (2014, October 22). Enabling blockchain innovations with pegged sidechains. Retrieved from <https://blockstream.com/sidechains.pdf>

Bellaire, M., Jaeger, J., & Len, J. (2017). Better than advertised: Improved collision-resistance guarantees for md-based hash functions. ACM SIGSAC Conference on Computer and Communications Security, (pp. 891-906). Dallas, TX.

Bryanov, K. (2019, June 30). Quantum computing vs. blockchain: Impact on cryptography. Retrieved from CoinTelegraph - The Future of Money: <https://cointelegraph.com/news/quantum-computing-vs-blockchain-impact-on-cryptography>

Chi, L., & Zhu, X. (2017). Hashing techniques: A survey and taxonomy. ACM Computing Surveys, 50(1), 11:1-11:36.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292 - 2303.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). COSO internal control - integrated framework: Internal control over external financial reporting. NY: COSO.

Cryptoticker. (2019, April 8). What is the blockchain data structure? Retrieved from Cryptoticker: <https://cryptoticker.io/en/blockchain-data-structure/>

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5-21.

Epoch Converter. (2019, April 8). EpochConverter. Retrieved from <https://www.epochconverter.com/>

Gervais, A., Ritzdorf, H., Karame, G. O., & Capkun, S. (2015). Tampering with the delivery of blocks and transactions in bitcoin. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 692-705). Denver: Association for Computing Machinery.

Hamer, J. (2002). Hashing revisited. Proceedings of the 7th Annual Conference on Innovation and Technology in Computer Science Education (pp. 80-83). Aarhus, DK: Association for Computing Machinery.

Haugen, R. (2002). The commitment oriented orchestration layer -- managing your business commitments. UN/CEFACT Quarterly Meeting, Seattle, WA.

He, D. (2018). Monetary policy in the digital age. *Finance & Development*, 55(2). Retrieved from International Monetary Fund.

Horiuchi, S., & McCarthy, W. E. (2011). An ontology-based state machine for catalog orders. Value Modeling and Business Ontologies Workshop. Ghent, BE.

Horiuchi, S., & Shimizu, X. (2016). Rethinking the development of a business process state machine. *Shogaku Ronsan*, 593-657.

Hussain, F. (2017). *Internet of things: Building blocks and business models*. Springer International Publishing.

International Organization for Standardization and the International Electrotechnical Commission . (2007). *ISO/IEC 15944-4 - Information technology - business operational view - part 4: business transaction scenarios - accounting and economic ontology*. Geneva, CH: International Standards Organization.

International Organization for Standardization and the International Electrotechnical Commission. (2019). *ISO/IEC 15944-21 Information technology - business operational view - part 21: guidance on the application of the open-edi business transaction ontology in distributed business transaction repositories (committee specification working draft)*. Geneva, CH: International Standards Organization.

Karame, G. O., Androulaki, E., & Capkun, S. (2012). Double-spending fast payments in bitcoin. *ACM conference on Computer and Communications Security* (pp. 906-). Raleigh: Association of Computing Machinery.

Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Capkun, S. (2012). Misbehavior in bitcoin: A study of double-spending. *ACM Transactions on Information and System Security*, 18(1), 2:1-2:32.

Kogan, A., Alles, M. G., Vasarhelyi, M. A., & Wu, J. (2014). Design and evaluation of a continuous data level auditing system. *Auditing: A Journal of Practice & Theory*, 33(4), 221-245.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart contracts smarter. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 254-269). Vienna: Association for Computing Machinery.

McCarthy, W. E., Geerts, G. L., & Gal, G. (2021). *The REA ontology*. Sarasota: American Accounting Association.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of bitcoins: characterizing payments among men with no names. *Communications of the ACM*, 59(4), 86-93.

Merkle, R. C. (1980). Protocols for public key cryptosystems. *IEEE Symposium on Security and Privacy* (pp. 132-145). Oakland, CA USA: IEEE.

Merkle, R. C. (1982). USA Patent No. US4309569.

National Institute of Standards and Technology. (2015). FIPS PUB 180-4 Secure hash standard (SHS). Gaithersburg, MD: National Institute of Standards and Technology.

Rittenberg, L. E., & Schwieger, B. (2001). *Auditing concepts for a changing environment* (Third ed.). New York: Harcourt, Inc.

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction. *International Conference on Financial Cryptography and Data Security* (pp. 6-24). Okinawa: Springer.

Sheehan, D., Gleasure, R., Feller, J., O'Reilly, P., Li, S., & Cristiforo, J. (2017). Does miner pooling impact bitcoin's ability to stay decentralized? *Proceedings of the 13th International Symposium on Open Collaboration*. Galway, IR: Association for Computing Machinery.

Tan, D., Hu, J., & Wang, J. (2019). VBBFT-Raft: An understandable blockchain consensus protocol with high performance. *7th International Conference on Computer Science and Network Technology* (pp. 111-115). Dalian: IEEE.

United States Congress. (2002). *Sarbanes-Oxley act*. Washington, DC: United States Congress.

Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. *Auditing: A Journal of Practice & Theory*, 10(1), 110-125.

Vukolić, M. (2017). Rethinking permissioned blockchains. *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (pp. 3-7). New York: Association for Computing Machinery.

Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30, 1-18.

Wirachantika, W., Barmawi, A. M., & Wahyudi, B. A. (2019). Strengthening fawkescoin against double spending attack using merkle tree. *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy* (pp. 49-54). Kuala Lumpur: Association for Computing Machinery.

Yang, S. (2018, February 21). The rise of bitcoin factories: Mining for the masses. *Wall Street Journal*.

Formatting Guide

MANUSCRIPT COMPONENTS

BAŞLIK (14pts, Center Text) (Turkish)

Name and Surname¹

Name and Surname²

ÖZ (12 pts, Text Left)

Maksimum 150 Kelime

Anahtar Kelimeler: En az 3 en fazla 5 kelime

JEL Sınıflandırması:

TITLE (14 pts, Center Text) (English)

ABSTRACT (12 pts, Text Left)

Maximum 150 Words

Keywords:

JEL Classification:

1 Academic Title, University, Faculty, Department, email, ORCID (10 pts., Times New Roman)

2 Academic Title, University, Faculty, Department, email, ORCID (10 pts., Times New Roman)

Extended Summary (Makalenin yazım dili Türkçe ise İngilizce olarak “extended summary” eklenmelidir.)

Introduction

Literature Review

Methodology

Conclusion

1. Introduction/Giriş (14pts, Text Left)

Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. (Comert, 2017)

Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. (Comert et al., 2018).

Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. (Comert, 2018; Tan, 2017; Kulah, 2015).

Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. (Gungor, 2017a).

Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. (Gungor, 2017b).

2. Literature Review/Literatur Taraması (14pts, Text Left)

Comert (2018) Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text.

Comert & Tan (2018) Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text.

Comert, Tan, & Sezer (2018) Text text text. Text text text. Text text text. Text text text. Text text text. Text text text.

Comert, Tan, Sezer, & Gungor (2018) Text text text. Text text text. Text text text. Text text text. Text text text. Text text text.

If the numbers of authors are five or more

Comert et al., (2018) Text text text. Text text text. Text text text. Text text text. Text text text. Text text text.

3. Methodology and Data/Metodoloji ve Data (14pts, Text Left)

3.1. Metodoloji (12pts, Text Left)

Equations and Formulas

$$CSAD_{i,t} = \alpha + (1-D)^{up} + y_{3D} + up(R_{m,t})^2 + (1-Dup)(R_{m,t})^2 + \epsilon_{ti} \quad (1)$$

$$T_i = (Rp - Rf) / p \quad (2)$$

where,

T_i = Treynor's performance index

R_p = Portfolio's actual return during a specified time period

R_f = Risk-free rate of return during the same period

3.2. Data (12pts, Text Left)

Text text text. Text text text. Text text text. Text text text. Text text text. Text text text.

4. Empirical Results/Analiz Sonuçları (14pts, Text Left)

Tables

Tables should appear within the text. Each table should be numbered consecutively. Tables must be numbered in the order in which they are to appear.

Table 1: List of Stock Exchanges

Country	List of Stock Exchanges	Starting Date	Ending Date	Obs. Days
Bahrain	Bahrain Stock Exchange	02.01.2003	31.08.2015	3302
Bangladesh	Dhaka Stock Exchange	01.01.1990	31.08.2015	6695
Abu Dhabi (Dubai)	Dubai Financial Market	02.01.2004	31.08.2015	3042
Egypt	Egyptian Exchange	02.01.1995	31.08.2015	5390
Indonesia	Jakarta Stock Exchange	02.01.1990	31.08.2015	6695
Jordan	Amman Stock Exchange	02.01.1990	31.08.2015	6695
Kuwait	Kuwait Stock Exchange	03.01.2000	31.08.2015	4086
Lebanon	Beirut Stock Exchange	01.02.1996	31.08.2015	5108
Malaysia	Bursa Malaysia	02.01.1990	31.08.2015	6695
Morocco	Casablanca Stock Exchange	02.01.2002	31.08.2015	3563
Oman	Muscat Securities Market	01.11.1996	31.08.2015	4912
Pakistan	Karachi Stock Exchange	02.01.1990	31.08.2015	6695
Qatar	Qatar Stock Exchange	01.09.1998	31.08.2015	4436
Saudi Arabia	Saudi Stock Exchange	02.11.1998	31.08.2015	4392
Tunisia	Tunis Stock Exchange	02.01.1998	31.08.2015	4607
Turkey	Borsa Istanbul	02.01.1990	31.08.2015	6695

Source:

Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text.

	Firm A	Firm B	Firm C
Constant	0.2085 (58.50)***	0.0150 (63.21)***	0.0192 (64.41)***
	0.0824 (2.27)**	0.3353 (16.86)***	0.2013 (7.54)***
$R^2_{m,t}$	2.1967 (3.21)***	1.8767 (4.77)***	0.0133 (0.0377)
Adj. R^2	0.1507	0.2373	0.2166

*, **, and **** represent statistical significance at the 10%, 5%, and 1% levels, respectively

Figures

Figures should appear within the text. Each figure should be numbered consecutively. Figures must be numbered in the order in which they are to appear. The term “figure” refers to a variety of material, including line drawings, maps, charts, graphs, photos, diagrams and photos.

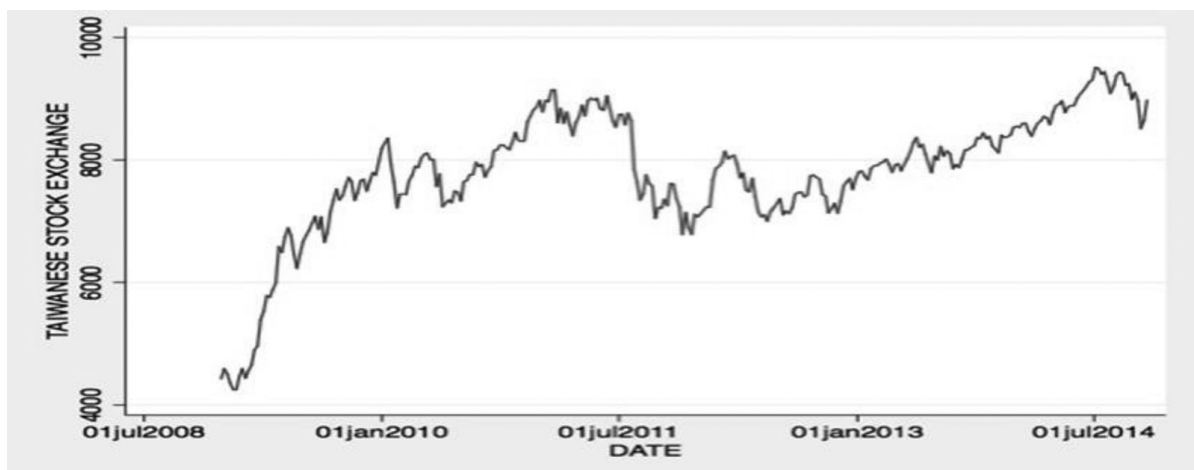


Figure 1: Daily Return of Taiwanese Stock Exchange

Source:

5. Conclusion/Sonuç (14pts, Text Left)

Text text text. Text text text. Text text text. Text text text. Text text text.
Text text text. Text text text. Text text text. Text text text. Text text text. Text text
text. Text text text. Text text text. Text text text. Text text text. Text text text. Text
text text. Text text text. Text text text. Text text text. Text text text. Text text text.
Text text text. Text text text. Text text text. Text text text. Text text text. Text text text.

ext text text. Text text text. Text text text. Text text text. Text text text. Text text text. Text text text.

Author Contribution/Yazar Katkısı

Tek yazarlı *çalışma* ise belirtmeye gerek yok

Conflict of Interest/Çıkar Çatışması

There is no conflict of interest among the authors.

“Yazarlar arasında *çıkar çatışması* yoktur” beyan edilmiştir. Tek yazarlı ise *çalışma* belirtmeye gerek

Financial Support/Finansal Destek

The author(s) has not received any financial support for this study

Eğer finansal destek alındıysa, desteğin alındığı kurum, proje numarası belirtilmelidir.

References/Kaynakça (10pts, Text Left, Alphabetic Order)

APA 6TH. edition

https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_formatting_and_style_guide/reference_list_articles_in_periodicals.html

(Please check the website)

Sample

Almeida, H., Campello, M., & Weisbach, M. S. (2004). The cash flow sensitivity of cash. *Journal of Finance*, 59(4), 1777–1804.

Bao, D., Chan, K. C., & Zhang, W. (2012). Asymmetric cash flow sensitivity of cash holdings. *Journal of Corporate Finance*, 18, 690–700. <https://doi.org/10.1016/j.jcorpfin.2012.05.003>.

Chen, D., Gan, C., Hu, B. (2013). *An empirical study of mutual funds performance in China*. Retrieved from <http://ssrn.com/abstract=2220323> or <http://dx.doi.org/10.2139/ssrn.2220323>.

Cleary, S. (1999). The relationship between firm investment and financial status. *Journal of Finance*, 54(2), 673–692.

Fazzari, S. M., Hubbard, R. G., Petersen, B. C., Blinder, A. S., & Poterba, J. M. (1988). Financing constraints and corporate investment. *Brookings Papers on Economic Activity*, 1988(1), 141–206.

Duncan, G. J., & Brooks-Gunn, J. (Eds.). (1997). *Consequences of growing up poor*. New York, NY: Russell Sage Foundation.

Resume/Özgeçmiş

1.Yazar

2.Yazar

Contents / İçindekiler

- 8 *Preface / Sunuş*
- 11 **Türk Bankacılık Sektörünün İç Sistemlerine Eleştirel Bir Yaklaşım**
A Critical Approach to the Internal Systems of the Turkish Banking Sector
Yağızcan Yücel ÇENDİK, Duygu ANIL KESKİN
- 41 **Muhasebe ve Denetimde Mesleki Yargının Epistemolojik Boyutu: Özne-Nesne İlişkisi**
Epistemological Dimensions of Professional Judgment in Accounting and Auditing: Subject-Object Relationship
Selahattin KARABINAR
- 55 **Using Big Data in Internal Fraud Detection**
İç Suîştimalin Tespitinde Büyük Verinin Kullanılması
Teoman Samet TEMUÇİN, Sefa ERBAŞ, Anıl AY
- 83 **Covid-19 Krizinde Sürdürülebilirlik Performansı ve Anormal Pay Getirisi Etkileri**
Sustainability Performance and Abnormal Stock Returns During the Covid-19 Crises
Emrah KELEŞ
- 103 **The External Financial Statement Audit Process and Blockchain Technology**
Finansal Tabloların Bağımsız Denetim Süreci ve Blokzincir Teknolojisi
Graham GAL, Matthew SHERWOOD
- 141 **Formatting Guide**

