Marmara Üniversitesi Öneri Dergisi • Cilt 15, Sayı 53, Ocak 2020, ISSN 2147-5377, ss. 254-275
DOI: 10.14783/maruoneri.676406

UYGULAMALI MAKALE/ APPLIED ARTICLE

CENTRAL AUDIT ACTIVITIES AS A CONTINUOUS AUDIT APPROACH IN THE TURKISH BANKING SECTOR: A CASE STUDY ABOUT FRAUDS IN SAVINGS ACCOUNTS

TÜRKİYE BANKACILIK SEKTÖRÜNDE BİR SÜREKLİ DENETİM YAKLAŞIMI OLARAK MERKEZDEN DENETİM: MEVDUAT HESAPLARINDAKİ HİLELER ÜZERİNE BİR VAKA ÇALIŞMASI

İsmail KABAN*

Abstract

Developments in information technology constitute the core of a fundamental transformation of internal audit approaches. The traditional concept of internal audit on periodic and traditional auditing with the inclusion of concepts such as data mining, artificial intelligence, and machine learning is replaced by modern continuous, risk-focused auditing. Recently, in sectors that have high transaction volume such as banking, continuous audit activities combined with data mining applications have become prominent in effectively managing fraud risk. In this study, an example of the examination process related to savings account fraud in Turkey has been presented by providing basic information about the central audit activities applied as a continuous audit approach in the banking sector. The banking transactions used as data in this fraud auditing were generated realistically and at random. Data mining techniques have been applied to these transactions to detect fraud risks.

Keywords: Internal Audit, Banking, Continuous Audit, Central Audit, Data Analytics.

JEL Classification: G21, M42

* Tokat Gaziosmanpaşa University, Department of Accounting and Tax Applications, E-mail:ismail_kaban@yahoo.com

Makale Gönderim Tarihi: 24.10.2019
Yayına Kabul Tarihi: 06.12.2019

Öz

Bilgi teknolojilerinde yaşanan gelişmeler iç denetim yaklaşımları üzerinde köklü bir dönüşümün çekirdeğini teşkil etmektedir. Veri madenciliği, yapay zekâ ve öğrenen makinalar gibi kavramların etkisi ile periyodik ve rutin denetimler üzerine kurgulanan geleneksel denetim anlayışının yerini sürekli ve risk odaklı modern denetim anlayışının aldığı görülmektedir. Son dönemde bankacılık gibi yüksek işlem yoğunluğu ihtiva eden sektörlerde suistimal risklerinin etkin olarak yönetilmesi için veri madenciliği uygulamaları ile harmanlanan sürekli denetim faaliyetleri öne çıkmaktadır. Bu çalışmada bankacılık sektöründe bir sürekli denetim yaklaşımı olarak uygulanan merkezden denetim faaliyetleri hakkında temel bilgiler sunularak Türkiye özelinde örnek bir mevduat suistimal vaka denetimi sürecine yer verilmiştir. Suistimal denetiminin gerçekleştirileceği işlemler gerçeğe uygun bir şekilde rastlantısal olarak üretilmiştir. Bu işlemler üzerinde veri madenciliği teknikleri uygulanarak hile risklerinin tespiti yapılmıştır.

Anahtar Kelimeler: İç Denetim, Bankacılık, Sürekli Denetim, Merkezden Denetim, Veri Analitiği.

Jel Kodları: G21, M42

1. INTRODUCTION

An enormous transformation in the world of internal audit has occurred with the evolution of information technology. The role of the banking sector has been strengthening in the global economy where radical financialization has taken place. This phenomenon enhances transaction volume in the banking sector and brings along additional fraud risks. These risks must be mitigated, as confidence in collecting deposits and credit processing has critical importance in terms of banking stability. Due to this increased transactional volume in the banking sector, conventional internal audit approaches are no longer sufficient with regards to managing fraud risks and providing efficiency in fraud audits. Through data mining techniques that were used in the audit process, a central audit activity enables the separation of high-volume data recorded by the banks on the basis of risky transactions. For this reason, the central audit shows itself as a strong tool for fraud detection and prevention. The central audit is a continuous audit approach focused on data analytics that allows auditing transactions instantaneously or very shortly after the execution of a fraud. Especially in sectors that have high transaction volume, such as banking, it is increasingly important to utilize the central audit.

The banking sector has a leading role in the use of information technologies. Accordingly, the banking sector is at the forefront of the sectors in which data production has risen day by day and reached very large volumes. The data produced in the banking sector has a variety ranging from the accounting records representing the realized transactions to the log records where all the digital movements are stored. In banking, almost all services are offered using software. This process results in the recording of each activity as well as the rapid and high-quality execution of processes. All records kept in the banks database have the characteristics of important inputs in organizing the business processes of the related departments. Therefore, it can be said that there are internal audit activities among the areas where these data sets can be used most effectively. It is of critical importance to analyze the data representing the customer transactions with certain techniques and to convert them into useful information to detect risky transactions and to prevent fraud attempts within the framework of risk-based audits. Data analytics and data mining applications are effective techniques used to transform data into meaningful information. The efficient data analytics and use of technological tools reduce operational costs in internal audit processes, as well as avoidance of reputation loss arising from fraud in banks.

The centralized audit is an internal audit approach that is used as a continuous audit model in the banking sector and makes it possible to perform audits on the databases where the activities carried out in the bank units are recorded. Therefore, thanks to centralized control, the activities carried out in these bank service units can be controlled remotely. In this respect, centralized control can also be considered a remote audit technique. In other words, central audit in the banking sector is a risk-based continuous audit approach based on computer-assisted audit techniques (CAATs). With CAATs and continuous audits, risk symptoms and abnormalities in operations can be easily detected. In contrast to the traditional audit, where the internal auditor assures the past, an instant and actual assurance is provided with the continuous audit. In other words, under the guidance of continuous audit, it is possible to determine the risks before the risks arise and to take the necessary precautions. In this respect, central audit as a continuous audit approach plays a vital role in occupational fraud audit processes in banking. In this study, specific to central audit as a continuous audit approach studies the banking sector in Turkey, specifically, the process of detecting embezzlement using SQL software is presented as a case study. The purpose of the study is to explain how the embezzlement is detected using SQL in the Turkish banking sector. It is thought that the study will contribute to the literature since no similar studies have been perfomed before.

2. LITERATURE REVIEW

The literature about central audit applications, data mining techniques or Computer Aided Audit Techniques (CAATs) in banks is limited. In this context, some academic studies on internal audit practices based on CAATs and data mining techniques in banks are presented below.

Debreceny, Lee, Neo and Shuling Toh (2005) evaluates the use of CAATs in financial institutions. In particular, this study reveals the nature of the Generalized Audit Software (GAS) practices used by the bank in internal and external audits. In this study, the interview method, which is a qualitative research technique was used. It has been observed that the scope and frequency of the use of GAS has changed substantially. According to the study, internal auditors see GAS as a tool for private investigations (e.g. fraud detection) rather than as a basis for regular audits.

Bologa, Bologa, and Florea (2013) aim to investigate the benefits of Big Data technology and the main methods of analysis that can be applied to the particular case of fraud detection in the public health insurance system in Romania. In this study, a qualitative research technique is used and the research is a case study. As a result, it has been determined that Big Data technologies will contribute to the effective detection of fraud in the health sector.

Teeter, Alles, and Vasarhelyi (2010) examine the concept of "remote control" as a process. The study was conducted in a theoretical framework. It is emphasized that internal auditors combine remote control with analytical procedures to gather electronic evidence, interact with the external auditor and report the accuracy of financial data and internal controls. According to the study, information, computing technologies, and data analytics provide remote work opportunities for internal auditors, reduce travel costs, and prevent late response to operations and increase efficiency and audit coverage.

Bhambri (2011) aims to highlights data mining applications in the banking sector. The study has a theoretical feature. This paper explains the fraud detection process as a tool used in data mining processes. According to the article, using data mining applications helps to identify the indicators that can lead to frauds.

Chitra and Subashini (2013) focus on data mining techniques and fraud prevention and detection in the banking sector. The study was conducted in a theoretical framework. According to the study, the customers with some demographics and transaction patterns are likely to misuse banks. The data mining technique helps to detect such symptoms that lead to fraud and to analyze processes.

Rahman and Anwar (2014) aim to present the perceptions of Islamic banking employees in Malaysia on the effectiveness of fraud prevention and detection techniques. In this study, a survey method a quantitative research technique was used. The results from the 146 questionnaires submitted from bank managers and officers indicate protection software/application as the most effective component of fraud prevention techniques.

Earley (2015) provides a background on the rise of Big Data and data analysis, a hot topic in the public accounting profession. The study has a theoretical feature. Despite the impression that data analytics is not easily accepted in auditing, public accounting firms continue to make significant investments in the development of data analytics related to the audit. It can be said that the transformational effect of these efforts will start to be seen over time.

The purpose of Tang, Norman and Vendrzyk's (2017) study is to understand the use of data analytics in the internal audit function and to investigate the types of tools that internal auditors use for analytical purposes by considering the big data. In this study, the interview method which is one of the qualitative research techniques was used. In this context, certified fraud examiners in both for-profit and not-for-profit organizations were interviewed. The findings show that certified fraud examiners value professional certification and data analytics. Certified fraud examiners report that they use data analytics techniques for different purposes and that a significant amount of budget is allocated to the internal audit to support this function.

These researches show that data analytics applications in the field of fraud auditing have started to be used in recent years and these applications have made significant contributions to fraud detection and prevention processes. Therefore, it can be said that the management of Big Data is critical today and in the future to combat fraud in sectors such as banking and insurance where a large volume transactions are performed.

3. THEORETICAL FRAMEWORK

This part provides theoretical information about internal audit, risk-focused internal audit, continuous audit and the relationship between internal audit and fraud within the framework of relevant literature.

3.1. Internal Audit And Risk Based Internal Audit

According to the definition by The Institute of Internal Auditors, internal audit is an independent, objective assurance and consulting function which aims to improve operations of an organization and add value to them. Internal audit contributes to the achievement of an organization's objectives by developing a systematic and disciplined approach to assessing and improving the effectiveness of risk management, control and governance processes (IIA, 2016, p.23). Within this scope when the role of internal audit is evaluated, internal audit as an activity providing independent, objective assurance and consulting about an organization's risk management, control, and corporate governance process. This contributes to the institutionalization of managerial accountability in businesses (Uzun, 2009, p.3). In this sense, the internal audit activity considers the following matters to assess the risks which are faced at the institution's governance processes, operations and information systems (IIA, 2016, pp.11-12):

- Achieving the strategic goals of the organization
- Reliability and accuracy of financial and operational information
- Effectiveness and efficiency of activities and programs
- Protection of assets
- Compliance with laws, regulations, policies, and agreements.

Table 1: The Shifting Focus of Internal Audit

The 20th-century internal audit model	Today's typical internal audit model	The risk-centric internal audit model of tomorrow
Controls assurance based on cyclical or routine audit plans	Controls assurance based on the risk-based internal audit plan	Assurance on the effectiveness of risk management in addition to controls assurance

Source: PWC, 2012, p. 2.

Risk-based internal audit is a methodology that associates all of the risk management work frames of an organization with an internal audit. A risk-based audit provides an internal audit structure that presents assurance to the board by establishing an effective risk management system based on the basis of risk appetite (CIIA, 2014, p. 1). Risk-based internal audit is an audit system that proposes to identify the risk factors concerning business processes, to measure the risk levels, to evaluate effectiveness and efficiency of controls to be applied regarding these risks and to prioritize the audits at areas that contain high-level risk (İDKK, 2013, p.180). Modern internal audit has replaced the traditional internal audit with a risk-based approach. Here, more important risks for the enterprise are identified. (Marks, 2015, p.18). Internal audit's focus has faced important changes from past to present (PWC, 2012, p.2). This change process is shown in the table above.

3.2. Continuous Audit

With the opportunities that are provided by information technology, incoming and outgoing documentation in classical internal audit has vanished and the scope of internal audit has turned into e-mail audits (Uzun, 2002, p.37). Manual controls run too late to prevent costly frauds, causing destructive reputation loss and negative financial results (Ramamoorti & Dupree, 2010, p.66). Since audit clients have increasingly refined their business systems from the documents, there is often no need to examine concrete paper and documents in audits today. Developed auditing software enables auditors to perform most of the audit methods on-line (Bierstaker, Burnaby & Thibodeau, 2001, p. 159). The transformation to electronic data warehouses and online simultaneous transactions from archiving documents by filing concretely has made serious anxiety in the mind of internal audit professionals (Liang , Lin & Wu, 2001, p. 130). Concerns that result from developments in information technologies are also related to risks with relevant upcoming technologies (Önce & İşgüden, 2012, p.50). Because information systems are widely utilized in the business world, various opportunities for deceptions has arisen from the point of the employee whithin a business and also people outside of a business (Hillison, Pacini, Sinason, Carson & Marlett, 2000, p.171). Therefore, rather than the mentality of reactive audit implementation, i.e. auditing some time after the operations are carried out, the continuous audit philosophy referring to audit concurrently with operations has come into practice.

The continuous audit is a wide electronic auditing process that makes it possible for auditors to supply some degree of assurance on information concurrently with, or shortly after, the disclosure of information (Rezaee, Sharbatoghlıe, Elam & Mcmickle, 2002, p.150). Technology has a key role in the continuous audit approach (Coderre, 2008, p. 70). The continuous auditing mentality in itself aims to provide assuring information that synchronously presented to the users by using advanced technology (Memiş & Tüm, 2011, p.149). This audit methodology is a combination of technology-based risk and control assessment. Business processes connected to continuous audit have been designed so that internal auditors can enable reporting about a topic in a much shorter time than a traditional retrospective approach (IIA, 2015, p.5).

3.2.1. Key Elements And Advantages of Continuous Audit

The continuous audit has two main parts, continuous risk assessment and continuous control assessment. Continuous risk assessment means the audit activities that determine and evaluate risk levels exist across the entity by assessing and comparing trends in processes and systems. When it comes to continuous control assessment, it means those audit activities evaluate weather selected controls are working properly or not (Coderre, 2007, pp.2-3). The situation of continuous control assessment and continuous risk assessment in a continuous audit model is shown the figure below. This model, which is called a continuous risk and control assurance model, has a function including continuous risk assessment and continuous control evaluation processes.

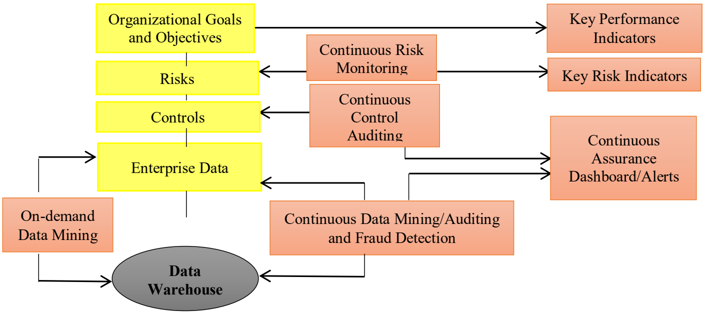

Organizational Goals and Objectives
Risks
Controls
Enterprise Data
Continuous Risk Monitoring
Continuous Control Auditing
Key Performance Indicators
Key Risk Indicators
Continuous Assurance Dashboard/Alerts
On-demand Data Mining
Continuous Data Mining/Auditing and Fraud Detection
Data Warehouse

Figure 1: Continuous Risk/Control Assurance Model

Source: Marks, 2010, p.3

In the above figure, two main components are becoming prominent in the form of continuous control audit and the continuous risk monitoring to attain organizational goals. Operational data stored in the data warehouse are used for continuous audit by using information technology. In the process of continuous audit, this data goes through the continuous control audit and the continuous risk monitoring phases. Through making necessary control and risk assessments in these phases, organizational goals are achieved. As mentioned above continuous audit consists of control, monitoring and assessment activities mainly implemented with information technology (Özbek, 2012, p.1028). As an example, payments to be made above a specific sum of money (15.000 TRY) to depositors after approval (maker/checker). The following steps shall be followed in the continuous audit activities on the internal control process designed for applying to secondary approval in these operations:

- Deposit payments above 15.000 TRY shall be extracted from data warehouse by using related software (continuous audit/continuous data mining),
- It shall be controlled whether there is a secondary approval given by the checker and whether this control point in the system is overridden in all of these transactions (continuous control audit) or not,
- Even though secondary approval is present at all transactions, it shall be evaluated whether approvals perform efficiently, for example, by establishing a controlled environment in which the passwords are not shared with others (continuous risk monitoring).
- After these related studies it can attain organizational goals.
- There are some essential components to run a continuous audit system. (Searcy, Woodroof & Colson, 2003, p. 46)
- The continuous audit environment typifies data exuded from the server system and the auditor's monitoring devices within the system.
- The continuous audit agreement is the contract between the parties participating in the continuous audit.
- The continuous audit is entirely dependent on the reliable functioning of interconnected systems.
- Transfer of information between the parties must be approved and supplied confidentiality, integrity, and authentication.
- When auditors access a web page in a continuous audit environment, they should be able to reach evergreen content.

Continuous audit activities improve organizations' internal audit processes and add value to internal audit operations. Based on this, the following advantages can be achieved by the use of internal audit practices in internal audit processes (O'Reilly, 2006, p.26):

- Building the audit process to be quicker, cheaper, more efficient, and more effective.
- Shortening audit frequencies to provide more well-timed risk and control assurance.
- Reaching greater audit coverage without the need to extend your resource base.
- Managing audits on a daily, monthly, or quarterly basis.

- Automating periodic audit testing and enhance audit frequency.
- Auditing 100 percent of data populations instead of just data samples.
- Matching and recalculating populations of data.
- Improving assurance quality as well as speed.

Fraud detection is one of the fields most preferred for continuous audit practices (Özbek, 2012, p. 1031). Continuous auditing can continuously test 100% of transactions in comparison to periodical auditing of a sample transaction group. For this reason, it changes the audit paradigm. The latest developments in information technology consist of the main reason that continuous auditing can be performed (TİDE, 2016, p.137).

3.2.2. Importance of Data in Continuous Audit and Data Mining

The first step to developing continuous audit methodology is reaching and understanding data (Coderre, 2007, p.2). The position of the data in the continuous audit process and its importance is shown below.

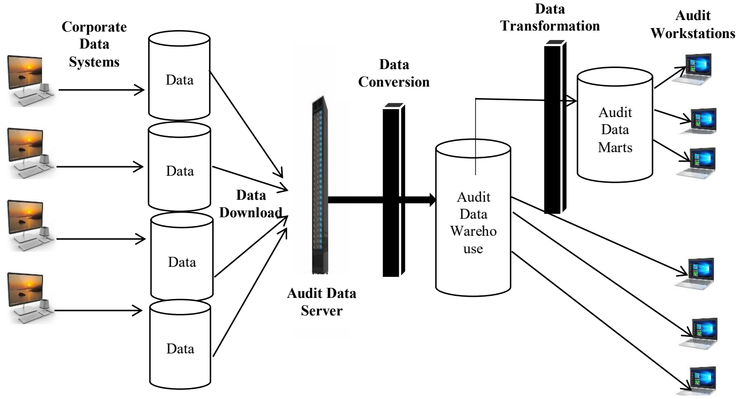


Figure 2: Example of A Continuous Audit Approach

Source: Rezaee, Sharbatoghlıe, Elam & Mcmickle, 2002, p.156

In the figure, it appears that all data generated in enterprise data systems are stored by transferring to the audit data server. The data gathered in the audit data server is subjected to some conversion operations so that the audit data warehouse is created. Finally, data in the related audit data warehouse is analyzed directly or after some processing to make it available to audit. Accordingly, the phases of data storage in a continuous audit are, confidentially, conversion, processing, and analysis of data.

In traditional internal audit activities, it is attempted to reach an opinion on the whole data set, especially by sampling huge data sets. However, with the support of continuous audit techniques such as data mining, it is possible to analyze the entire data set, even if it is very large (Özbek, 2012, pp.1031-1032).

Data mining is one of the techniques utilized at the center of continuous audit operations. Data mining as a proactive audit technique is utilized while performing audits by internal auditors with relation to misappropriation of assets (e.g. embezzlements in banks) and information misrepresentation (IIA, 2009, p.11). Data mining is one of the data analytics techniques commonly used for fraud detection. The data mining concept has a key role in a comprehensive fraud audit system (CIMA, 2009, p.24). But data mining is a technique that produces alarms regarding fraud attempts rather than detecting the fraud directly (Buoni, 2012, p.37). Intuitions have an important role in data mining; because anomalies or exceptions to them can be completely harmless and can be verified in this way (Golden, Steven & Mona, 2006, p.386), auditors need to use professional reasoning power to examine the anomalies and sample data (Vona, 2008, p.70). The significant advantage of data analysis technology is that it addresses the specific needs of the auditor when detecting indicators of fraudulent activity (IIA, 2011, p.9). With data analysis, data mining and digital analysis tools, it is possible to identify suspicious transactions, monitor fraud threats, and vulnerabilities, and analyze thousands or millions of transactions (IIA, AICPA & ACFE, 2008, pp.36-37). The findings obtained by applying data mining techniques have never been able to provide complete assurance of the accuracy of the fraud directly. Data mining does, however, allow the auditor to conduct risk-based and proactive audits using professional judgment on the findings obtained.

3.3. Central Audit in Banks

Continuous audit, called central audit or remote audit in banks, has developed to a great extent to help financial institutions assess the risks in branch networks in particular. Central audit as a continuous audit approach in banks is an audit methodology developed to control records through the bank database. It is aimed to prevent potential risks with data analysis/interpretations made within the scope of central audit activities and to contribute more to the proactive audit approach (ZB, 2008, p.56). The core of central audit activities is based on computer-assisted auditing techniques (CAAT) (VB, 2016, p.103). Remote audit studies give an opportunity to consistently monitor very risky fields, notably credit and human resources areas (İB, 2016, p.77). The following operations are carried out within the scope of central audit activities (HB, 2016, p.124):

- Early detection of possible fraud and operational errors by concentrating on transactions with high-risk levels.
- Establishment and examination of various risk reports protecting the interests of depositors and bank shareholders.

Central audit operations with remote monitoring techniques are executed to determine the problems in processes and applications and to provide coordination with interested parties for taking action by analyzing customer complaints (GB, 2016, p.126). All documents are archived in systematic databases, the so-called the operations center, which is carried out in banks with the help of information processing technology. This phenomenon contributes to developing central audit implementations day by day. Through scenario analysis designed within the frame of central audit implementation, not only actual frauds may be detected, but also there is a deterrent effect in terms of preventing possible irregularities. Within the context of remote audit operations, existing scenarios' efficiency is permanently reviewed and new scenarios are created against potential irregularities by evaluating new business processes, systematic improvements are made to minimize manual process-related risks that are used in audit process (ZB, 2016, p.74).

The following activities are carried out by the central auditing activities (HB, 2009, p.80):

- Gain instant control of risky operations.
- Identification of possible irregularities in the earliest time and without much damage.
- Standardization of internal audit activities.
- Improvement of site audits' quality and efficiency.
- Decrease the time of site audits which are performed in branch, unit, and subsidiaries.
- Concentration of risky transactions as part of risk-based audit concept.

Scenarios are created based on a specific risk set up within the frame of central audit activities. Analysis and scenario development processes are mainly in the form of brainstorming sessions. Scenarios obtained in the result of these brainstorming sessions are formulated by using a business intelligence software (ACL etc.). These formulas are implemented onto data from the unit to be audited. Risky operations are detected by applying data mining techniques on account transactions and logs regarding all transactions performing in the bank. Thereby concurrent audits may be executed without having to go to any place. Thus, for example, deposit and credit transactions which are fulfilled in branch can be permanently monitored.

3.4. Relationship Between Internal Audit And Fraud

Since it is difficult to detect fraud, internal auditors try to develop different methods over time. Concordantly, proactive methods have crucial importance in immediately detecting the presence of fraud and avoiding damage before reaching important levels (Çatıkkaş & Çalış, 2010, p.156).

The internal auditor who implements a proactive method doesn't wait for the realization of fraud or the emergence of a sign of fraud. Internal auditor tries to figure out the type of frauds that can be done in the organization and the possible clues about these kinds of frauds. Then internal auditor examines whether there are these kinds of symptoms in the entity. In this approach, which can also be considered as a hypothesis testing approach, the internal auditor creates a hypothesis and scrutinizes whether each one of the hypotheses is confirmed. When proactive methods are used to detect frauds, the greatest achievement is that the fraud is detected before it becomes actual (Albrecht, Albrecht, Albrecht & Zimbelman, 2012, p.169). Data mining is an effective technique for proactive internal audit and fraud audits (Giles, 2012, p.250).

There is no definite expectation from internal auditors to detect fraud and violations. (Musa, 2017, p.32). However, internal auditors analyze and evaluate whether there are risk elements such as pressure, opportunity, and rationalization in their audits. These evaluations are substantially carried out on the basis of auditors' professional judgment (Mengi, 2012, p.123).

Nowadays, internal auditors should prioritize proactive approaches as they perform audit functions. Thus it will be possible to efficiently grapple with fraud (Çatıkkaş & Çalış, 2010, p.156). The average loss that occurs on the basis of fraud types has significantly decreased in the last decade. Average losses that appear in the form of asset misappropriation, corruption and financial statement frauds decreased from $150,000, $538,000 and $2,000,000 in 2006 to $125,000, $200,000 and $1,000,000 in 2016 respectively (ACFE, 2006, p.10; ACFE, 2016, p. 12). This particularly significant decrease which takes place on the basis of corruption and financial statement fraud is noteworthy. This proves that the developments in the internal audit function had a deterrent effect on the fraud.

Today expectations about the prevention, detection, and reporting of frauds from internal audit units are even higher than that were in the past. But, organizations should not always expect internal audit to have the fraud investigation skills. Instead, internal audit should support the organization's anti-fraud management efforts by providing necessary assurance services over internal controls designed to detect and prevent fraud. However, if an internal audit is required to investigate fraud, the internal auditor should have the necessary skills and experience to investigate within the framework of his / her professional responsibilities. The internal auditor should not endanger the investigation and relevant evidence in this process (IIA, 2019, p.3). Some internal auditors can be trained on fraud types and subjected to certificate programs to give them the ability to combat fraud more effectively. Thus, internal auditors who gain expertise in fraud can successfully fulfill positive fraud audit outcomes in the entity.

4. A DETERMINATION BY CONTINUOUS AUDIT APPROACH BASED DATA MINING ON A POSSIBLE FRAUD CONCERNING THE BANKING SECTOR; A CASE STUDY

This chapter focused on embezzlement acts, the most common type of fraud in the Turkish banking sector. A case study on the detection of embezzlement actions using data mining techniques is presented. In this direction, a high number of banking transactions, which were randomly and realistically generated, were considered. It is demonstrated how to use the SQL programming language to detect transactions that are considered risky. In the central audit processes, the unusual transactions diverging from the routine operations of the customers are defined as risk factors. These transactions are considered abnormal and are referred to as 'scenarios' in the central audit work. These processes are converted into query language using SQL. Thus, it is possible to detect the corresponding process from a very high number of data in a very short time. The following steps were followed during the preparation of this case study;

a. Production of a large number of proper data (30,000 customer transactions).

b. An embezzlement action scenario with high probability.

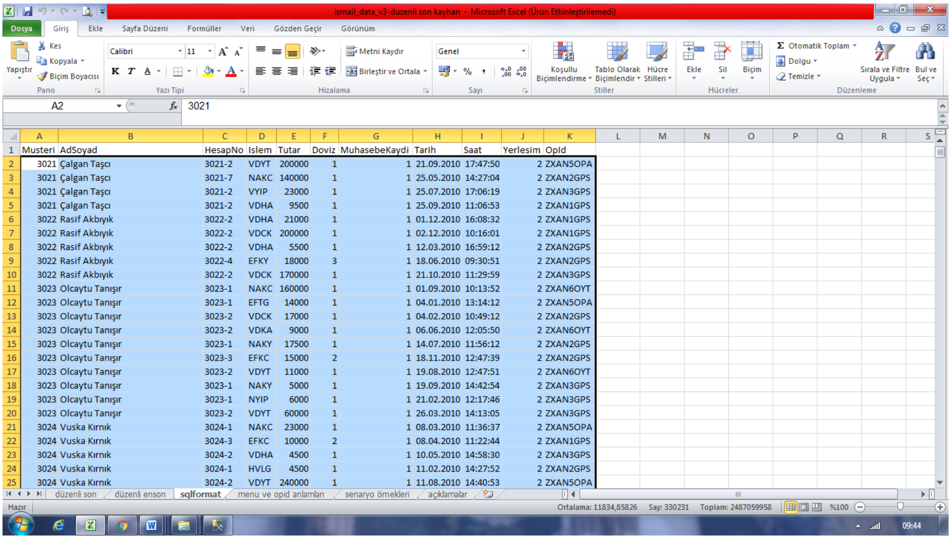
c. Transformation of the central audit scenario into SQL query language as a data mining method.

d. Discovering related processes in the database by running SQL queries.

Descriptions of the above steps are respectively listed below.

4.1. Producing A Large Number of Realistic Data

Thousands of transactions are carried out in branches as the most widespread service units of the banks every day. Almost all of them are in the structure of credit and deposit transactions. In this direction, more than 330,000 data were produced so as to mirrorr the transactions that were established on a day to day basis in a bank and the database for the case study was created. Microsoft Excel was used in the data production process. This database represents more than 30,000 banking transactions. The Excel and SQL screenshots for the generated database are presented below.

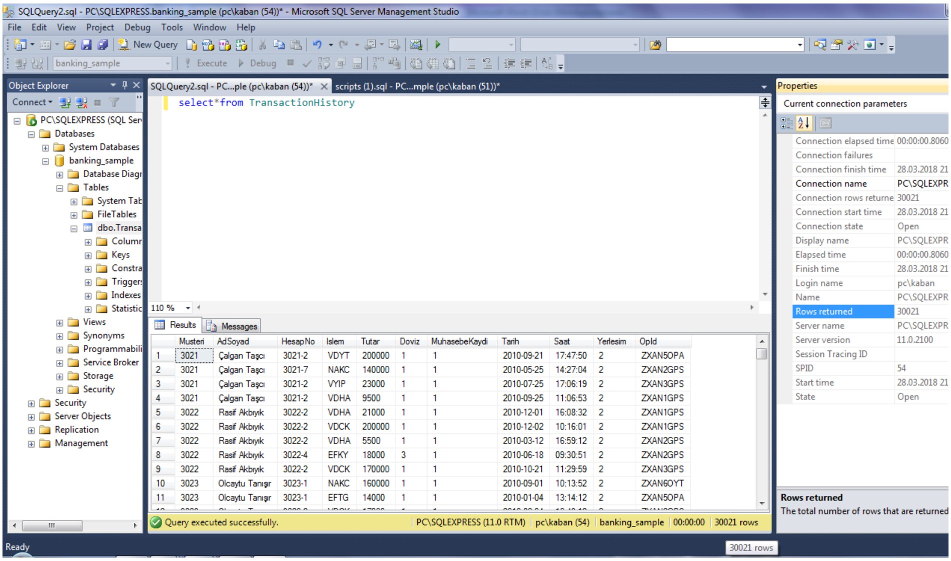


A2 = 3021

	A	B	C	D	E	F	G	H	I	J	K
1	Musteri	AdSoyad	HesapNo	Islem	Tutar	Doviz	MuhasebeKaydi	Tarih	Saat	Yerlesim	OpId
2	3021	Çalgan Taşcı	3021-2	VDYT	200000	1	1	21.09.2010	17:47:50	2	ZXAN5OPA
3	3021	Çalgan Taşcı	3021-7	NAKC	140000	1	1	25.05.2010	14:27:04	2	ZXAN2GPS
4	3021	Çalgan Taşcı	3021-2	VYIP	23000	1	1	25.07.2010	17:06:19	2	ZXAN3GPS
5	3021	Çalgan Taşcı	3021-2	VDHA	9500	1	1	25.09.2010	11:06:53	2	ZXAN1GPS
6	3022	Rasif Akbıyık	3022-2	VDHA	21000	1	1	01.12.2010	16:08:32	2	ZXAN1GPS
7	3022	Rasif Akbıyık	3022-2	VDCK	200000	1	1	02.12.2010	10:16:01	2	ZXAN1GPS
8	3022	Rasif Akbıyık	3022-2	VDHA	5500	1	1	12.03.2010	16:59:12	2	ZXAN2GPS
9	3022	Rasif Akbıyık	3022-4	EFKY	18000	3	1	18.06.2010	09:30:51	2	ZXAN2GPS
10	3022	Rasif Akbıyık	3022-2	VDCK	170000	1	1	21.10.2010	11:29:59	2	ZXAN3GPS
11	3023	Olcaytu Tanışır	3023-1	NAKC	160000	1	1	01.09.2010	10:13:52	2	ZXAN6OYT
12	3023	Olcaytu Tanışır	3023-1	EFTG	14000	1	1	04.01.2010	13:14:12	2	ZXAN5OPA
13	3023	Olcaytu Tanışır	3023-2	VDCK	17000	1	1	04.02.2010	10:49:12	2	ZXAN2GPS
14	3023	Olcaytu Tanışır	3023-2	VDKA	9000	1	1	06.06.2010	12:05:50	2	ZXAN6OYT
15	3023	Olcaytu Tanışır	3023-1	NAKY	17500	1	1	14.07.2010	11:56:12	2	ZXAN2GPS
16	3023	Olcaytu Tanışır	3023-3	EFKC	15000	2	1	18.11.2010	12:47:39	2	ZXAN2GPS
17	3023	Olcaytu Tanışır	3023-2	VDYT	11000	1	1	19.08.2010	12:47:51	2	ZXAN6OYT
18	3023	Olcaytu Tanışır	3023-1	NAKY	5000	1	1	19.09.2010	14:42:54	2	ZXAN3GPS
19	3023	Olcaytu Tanışır	3023-1	NYIP	6000	1	1	21.02.2010	12:17:46	2	ZXAN3GPS
20	3023	Olcaytu Tanışır	3023-2	VDYT	60000	1	1	26.03.2010	14:13:05	2	ZXAN3GPS
21	3024	Vuska Kırnık	3024-1	NAKC	23000	1	1	08.03.2010	11:36:37	2	ZXAN5OPA
22	3024	Vuska Kırnık	3024-3	EFKC	10000	2	1	08.04.2010	11:22:44	2	ZXAN1GPS
23	3024	Vuska Kırnık	3024-2	VDHA	4500	1	1	10.05.2010	14:58:30	2	ZXAN3GPS
24	3024	Vuska Kırnık	3024-1	HVLG	4500	1	1	11.02.2010	14:27:52	2	ZXAN2GPS
25	3024	Vuska Kırnık	3024-2	VDYT	240000	1	1	11.08.2010	14:40:53	2	ZXAN5OPA

Figure 3. Realistically Produced Banking Transaction Data

The necessary processing is done on the produced data with Excel and this data is made compatible with the SQL query. As shown in Figure, 30.021 banking transactions have been produced in accordance with reality.



```
select*from TransactionHistory
```

	Musteri	AdSoyad	HesapNo	Islem	Tutar	Doviz	MuhasebeKaydi	Tarih	Saat	Yerlesim	OpId
1	3021	Çalgan Taşcı	3021-2	VDYT	200000	1	1	2010-09-21	17:47:50	2	ZXAN5OPA
2	3021	Çalgan Taşcı	3021-7	NAKC	140000	1	1	2010-05-25	14:27:04	2	ZXAN2GPS
3	3021	Çalgan Taşcı	3021-2	VYIP	23000	1	1	2010-07-25	17:06:19	2	ZXAN3GPS
4	3021	Çalgan Taşcı	3021-2	VDHA	9500	1	1	2010-09-25	11:06:53	2	ZXAN1GPS
5	3022	Rasif Akbıyık	3022-2	VDHA	21000	1	1	2010-12-01	16:08:32	2	ZXAN1GPS
6	3022	Rasif Akbıyık	3022-2	VDCK	200000	1	1	2010-12-02	10:16:01	2	ZXAN1GPS
7	3022	Rasif Akbıyık	3022-2	VDHA	5500	1	1	2010-03-12	16:59:12	2	ZXAN2GPS
8	3022	Rasif Akbıyık	3022-4	EFKY	18000	3	1	2010-06-18	09:30:51	2	ZXAN2GPS
9	3022	Rasif Akbıyık	3022-2	VDCK	170000	1	1	2010-10-21	11:29:59	2	ZXAN3GPS
10	3023	Olcaytu Tanışır	3023-1	NAKC	160000	1	1	2010-09-01	10:13:52	2	ZXAN6OYT
11	3023	Olcaytu Tanışır	3023-1	EFTG	14000	1	1	2010-01-04	13:14:12	2	ZXAN5OPA

Query executed successfully. | PC\SQLEXPRESS (11.0 RTM) | pc\kaban (54) | banking_sample | 00:00:00 | 30021 rows

30021 rows

Properties

Current connection parameters

Connection elapsed time	00:00:00.8060
Connection failures	
Connection finish time	28.03.2018 21
Connection name	PC\SQLEXPR
Connection rows returne	30021
Connection start time	28.03.2018 21
Connection state	Open
Display name	PC\SQLEXPR
Elapsed time	00:00:00.8060
Finish time	28.03.2018 21
Login name	pc\kaban
Name	PC\SQLEXPR
Rows returned	30021
Server name	PC\SQLEXPR
Server version	11.0.2100
Session Tracing ID	
SPID	54
Start time	28.03.2018 21
State	Open

Rows returned
The total number of rows that are returned

Figure 4. Transmission Of Banking Transaction Data To SQL Program

4.2. An Embezzlement Scenario Which Can Be Used in The Central Audit

This case study is based on an embezzlement scenario in the form of Payment from Savings Account “A” Belonging to “X” – Repayment from Savings Account “A” Belonging to “X” in Same Day. In the case of this potential fraudulent transaction, it is assumed that bank personnel has suspicious transactions on the account of a customer with a savings account in the branch. In this case, the bank personnel may have paid less amount than the interest income on the account to the customer at the bank branch. Thus, the employee may have used the confidence that the client has felt for him and in fact, he may have paid a lower amount than the interest income and have embezzled the rest of the accrued interest. Logically, repeated withdrawals from past due accounts on the same day is a rare situation. For this reason, such transactions are likely to be fraudulent.

4.3. Transformation of The Central Audit Scenario Into Sql Query Language As A Data Mining Tool

The SQL query of an embezzlement scenario in the form of Payment from Savings Account “A” Belonging to “X” – Repayment from Savings Account “A” Belonging to “X” in Same Day is below.

SQL Query:

select a.Musteri, a.AdSoyad, a.Islem, a.Tutar, a.Tarih, a.Saat, a.OpId, b.Musteri, b.AdSoyad, b.Islem, b.Tutar, b.Tarih, b.Saat, b.OpId from TransactionHistory a, TransactionHistory b

Where a.Islem = ‘VDCK’ and b.Islem = ‘VDCK’ and a.Musteri = b.Musteri and a.Tarih = b. Tarih and a.OpId = b.OpId and a.Doviz = b.Doviz and a.Saat < b.Saat

The English translation of the SQL query is as follows:

SQL Query as English:

select a.Customer, a.NameSurname, a.Transaction, a.Amount, a.Date, a.Time, a.OpId, b. Customer, b. NameSurname, b.Transaction, b.Amount, b.Date, b.Time, b.OpId from TransactionHistory a, TransactionHistory b

Where a.Transaction = ‘VDCK’ and b.Transaction = ‘VDCK’ and a.Customer = b.Customer and a.Date = b. Date and a.OpId = b.OpId and a.Currency = b.Currency and a.Time < b. Time

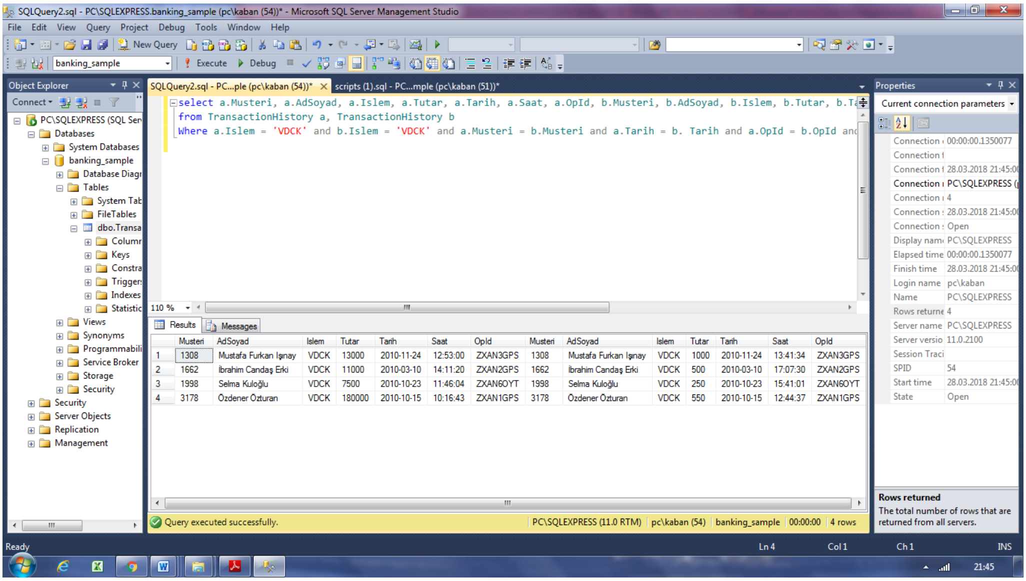
In the above SQL query, an assembly that satisfies all of the following points has been formulated:

- Both a and b transactions have the characteristic of VDCK (withdrawal of savings deposits) (a.Islem = ‘VDCK’ and b.Islem = ‘VDCK’),

- The customer is the same person in both processes (a.Musteri = b.Musteri).
- The date is the same date in both processes (a.Tarih = b. Tarih).
- Both transactions are carried out by the same employee of the bank (a.OpId = b.OpId).
- The currency is the same currency in both processes (a.Doviz = b.Doviz).
- The first operation time is tearlier than the second operation time (a.Saat < b.Saat).

4.4. Discovering Related Transactions in The Database By Running SQL Queries

The following results have been obtained after running the scenario converted to SQL query in the database. Screenshots of related records are presented below.



SQLQuery2.sql - PC\SQLEXPRESS.banking_sample (pc\kaban (54))* - Microsoft SQL Server Management Studio
File Edit View Query Project Debug Tools Window Help
New Query
banking_sample
Execute
Debug
Object Explorer
SQLQuery2.sql - PC...ple (pc\kaban (54))*
scripts (1).sql - PC...mple (pc\kaban (51))*
Properties
Current connection parameters

```sql
select a.Musteri, a.AdSoyad, a.Islem, a.Tutar, a.Tarih, a.Saat, a.OpId, b.Musteri, b.AdSoyad, b.Islem, b.Tutar, b.Ta
from TransactionHistory a, TransactionHistory b
Where a.Islem = 'VDCK' and b.Islem = 'VDCK' and a.Musteri = b.Musteri and a.Tarih = b. Tarih and a.OpId = b.OpId and
```

	Musteri	AdSoyad	Islem	Tutar	Tarih	Saat	OpId	Musteri	AdSoyad	Islem	Tutar	Tarih	Saat	OpId
1	1308	Mustafa Furkan Işınay	VDCK	13000	2010-11-24	12:53:00	ZXAN3GPS	1308	Mustafa Furkan Işınay	VDCK	1000	2010-11-24	13:41:34	ZXAN3GPS
2	1662	İbrahim Candaş Erki	VDCK	11000	2010-03-10	14:11:20	ZXAN2GPS	1662	İbrahim Candaş Erki	VDCK	500	2010-03-10	17:07:30	ZXAN2GPS
3	1998	Selma Kuloğlu	VDCK	7500	2010-10-23	11:46:04	ZXAN6OYT	1998	Selma Kuloğlu	VDCK	250	2010-10-23	15:41:01	ZXAN6OYT
4	3178	Özdener Özturan	VDCK	180000	2010-10-15	10:16:43	ZXAN1GPS	3178	Özdener Özturan	VDCK	550	2010-10-15	12:44:37	ZXAN1GPS

```
Query executed successfully.   PC\SQLEXPRESS (11.0 RTM) | pc\kaban (54) | banking_sample | 00:00:00 | 4 rows
```

Figure 5. Execution Of SQL Query on Banking Transaction Data

The SQL screenshot above shows the records obtained as a result of running the relevant scenario. Accordingly, the transaction couple was discovered related to the scenarios defined as a fraud risk factor in the data of 30021 rows. Thousands of data points have been queried within seconds with the data mining technique applied using the SQL program and the fraud risks have been revealed. These transactions are shown below.

Table 2: Risk Records Obtained as A Result of SQL Query

Musteri (Customer)	**AdSoyad (NameSurname)**	**Islem (Transaction)**	**Tutar (Amount)**	**Tarih (Date)**	**Saat (Time)**	**OpId**	**Doviz (Currency)**
1308	Mustafa Furkan Işınay	VDCK	13000	24.11.2010	12:53:00	ZXAN3GPS	1
1308	Mustafa Furkan Işınay	VDCK	1000	24.11.2010	13:41:34	ZXAN3GPS	1
1662	İbrahim Candaş Erki	VDCK	11000	10.03.2010	14:11:20	ZXAN2GPS	1
1662	İbrahim Candaş Erki	VDCK	500	10.03.2010	17:07:30	ZXAN2GPS	1
1998	Selma Kuloğlu	VDCK	7500	23.10.2010	11:46:04	ZXAN6OYT	1
1998	Selma Kuloğlu	VDCK	250	23.10.2010	15:41:01	ZXAN6OYT	1
3178	Özdener Özturan	VDCK	180000	15.10.2010	10:16:43	ZXAN1GPS	1
3178	Özdener Özturan	VDCK	550	15.10.2010	12:44:37	ZXAN1GPS	1

The data presented in the above table indicate that consecutive payments are made from customers' savings account within the same day. Accordingly, these transactions mean the following:

- 13.000 TRY had been paid from Mustafa Furkan Işınay's savings account by the ZXAN3GPS user code on 24.11.2010 at 12:53 and 1.000 TRY at 13:41.
- 11.000 TRY had been paid from İbrahim Candaş Erki's savings account by the ZXAN2GPS user code on 10.03.2010 at 14:11 and 500 TRY at 17:07.
- 7.500 TRY had been paid from Selma Kuloğlu's savings account by the ZXAN6OYT user code on 23.10.2010 at 11:46 and 250 TRY at 15:41.
- 180.000 TRY had been paid from Özdener Özturan's savings account by the ZXAN-1GPS user code on 15.10.2010 at 10:16 and 550 TRY at 12:44.

After the execution of SQL queries, the records must be examined in detail. In other words, it is necessary to further investigate the existence of a possible act of embezzlement in these transactions. Some studies to be done in this direction are as follows:

- If there is no customer signature on the receipt belonging to the second transaction, the conclusion will be that the transaction is not made by the customer. This transaction will be deemed to be fraudulent and employee's other actions will be examined in detail by interrogation of the relevant personnel. If the employee confesses to his/her offense, a handwritten confession will be taken and the examination will be deepened.

- If there is a signature on the receipt belonging to the second transaction, it will be checked whether the signature belongs to the customer. If there is any suspicion that the signature belongs to the customer, an interview will be held with the customer to decide whether or not he/she has done this. If the customer declares that he/she has not done the transaction, personnel will be interrogated and attempts to reveal the actual nature of the transaction shall be made. If an employee confesses to anoffense, a handwritten confession will be taken and further investigation is required. If the personnel does not make a confession, the corresponding receipts will be sent to the criminological examination to determine whether the signature on the receipts belongs to the customer. In the light of criminological results, examination methods will be determined.

- Even if there is a customer's signature on the receipt regarding the second transaction, if the employee performing the transaction exhibits suspicious behavior, the receipt concerning that transaction may have been previously unsigned. From this point of view, an interview will be carried out with the customer to find out whether the transaction was, in fact, performed by the customer.. If the customer declares that they have not done this transaction, the employee will be interviewed iin an attempt to reveal the true nature of the transaction.. If there are blnk, unsigned receipt forms belonging to other customers oin the employees possession, this will increase the suspicion on the employee. If an employee confesses to an offense, a handwritten confession will be taken and further examination will take place.

5. CONCLUSION

The central audit activities are aimed at determining situations that are divergent from routine banking transactions, which are called "scenarios". In other words, central audit activities focus on identifying transactions that are outside of the behavioral patterns that a customer would follow in an ordinary bank-customer relationship. Thus, out-of-the-norm operations are instantaneously detected using data mining techniques and fraudulent actions are effectively dealt with.

Central auditing provides a high level of efficiency in the fraud prevention processes of banks on the basis of the continuous audit methodology. While fraud prevention is based on a predominantly reactive approach in classical internal audit, the central audit is proactive in nature. Thus, it becomes possible to detect frauds before they take place or immediately after they occur.

The findings of this study show that accounting transactions that are suspected of embezzlement among the mass data in the banking sector, as a sector where excessively transactions are performed, can be easily identified by using these data analytical techniques. In the study, 4 fraud schemes with embezzlement indications were determined among 30021 data. In this respect, it can be said that data analysis techniques are critical in detecting fraud risks with a risk-oriented fraud audit approach. Data analytics applications, one of the most important functions of generalized audit software, enable effective fraud struggle with limited audit resources. The cost of time and human resources for the 30,021 data presented in the study can be minimized by data analytical techniques. In addition, it can be said that the examinations carried out on 4 fraud schemes detected in the study and which have a relatively higher fraud risk potential will contribute to the effectiveness and efficiency of fraud audit activities.

Concepts such as Big Data, artificial intelligence, machine learning and industry 4.0 are at the center of intense interest today. These concepts carry business processes and job descriptions to the brink of a great change. There is a serious transformation under the influence of these developments both in internal audit processes and internal audit profession. Central auditing is gaining ground as a reflection in the banking sector of the lights-out/unmanned factories paradigm seen in the production sector. In this respect, central auditing points to the starting point of the internal audit activity to be carried out as unmanned, as well a, with the production to be made in the unmanned factory. Therefore, it can be said that an analogy for internal audit of the industry 4.0 concept, which centered on unmanned factories in production, is the unmanned audit. Thus, it is possible to combat mass transactions through an effective fraud prevention model, where central auditing takes place in the core.

REFERENCES

Albrecht, Steve W., Albrecht, Chad O., Albrecht, Conan C. & Zimbelman, Mark F. (2012). *Fraud Examination.* USA: South-Western, Cengage Learning.

Associaiton of Certified Fraud Examiners (ACFE) (2006). *Report to the nations on occupational* fraud *and abuse*. Retrieved from https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/2006-rttn.pdf

Associaiton of Certified Fraud Examiners (ACFE) (2016). *Report to the nations on occupational fraud and abuse 2016 global fraud study*. Retrieved from https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

Bhambri, V. (2011). Application of data mining in banking sector. *International Journal of Computer Science and Technology,* 2 (2), 199-202.

Bierstaker, J. L., Burnaby, P. & Thibodeau, J. (2001). The impact of ınformation technology on the audit process: an assessment of the state of the art and ımplications for the future. *Managerial Auditing Journal,* 16 (3), 159-164.

Bologa, A. R., Bologa, R. & Florea, A. (2013). Big data and specific analysis methods for insurance fraud detection. *Database Systems Journal*, 4 (4), 30-39.

Buoni, A. (2012). *Fraud Detection in The Banking Sector*. Turku: TUCS.

Chartered Instıtute of Internal Audıtors (CIIA) (2014). *Risk Based Internal Auditing.* London. Retrieved from https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf

Chitra, K. & Subashini, B. (2013). Data mining techniques and its applications in banking sector. *International Journal of Emerging Technology and Advanced Engineering,* 3(8), 219-226.

Coderre, D. (2007). Recommendations for an effective continuous audit process. *Internal Auditor*, *17, 1-7*.

Coderre, D. (2008). *Internal Audit: Efficiency Through Automation*. New Jersey: John Wiley & Sons.

Çatıkkaş, Ö. & Çalış, Y. E. (2010). Hile denetiminde proaktif yaklaşımlar. *Muhasebe ve Finansman Dergisi,* 45, 146-156.

Debreceny, R., Lee, S. L., Neo, W. & Shuling Toh, J. (2005). Employing generalized audit software in the financial services sector: challenges and opportunities. *Managerial Auditing Journal,* 20(6), 605-618.

Earley, C. E. (2015). Data analytics in auditing: opportunities and challenges. *Business Horizons,* 58(5), 493-500.

Garanti Bank (GB) (2016). *2015 annual report*. İstanbul. Retrieved from https://www.garantibbvainvestorrelations.com/en/images/pdf/Garanti-Bank-2015-Annual-Report.pdf

Giles, S. (2012). *Managing Fraud Risk: A Practical Guide for Directors and Managers*. United Kingdom: John Wiley & Sons.

Golden, T. W., Steven L. S. & Mona, M. C. (2006). *A Guide To Forensic Accounting Investigation*. New York: John Wiley & Sons.

Hillison, W., Pacini, C., Sinason, D., Carson, J. M. & Marlett, D. C. (2000). The insurance firm internal auditor as fraud-buster. *CPCU Journal,* 53(3), 168-180.

İç Denetim Koordinasyon Kurulu. (İDKK) (2013). *Kamu Iç Denetim Rehberi*. Ankara.

Liang, D., Lin, F. & Wu, S. (2001). Electronically auditing EDP systems: With the support of emerging information technologies. *International Journal of Accounting Information Systems,* 2 (2), 130-147.

Marks, N. (2010). Continuous auditing reexamined. *ISACA Journal,* 1, 1-5

Marks, N. (2015). Modern Risk-Based Internal Auditing. *Internal Auditor-Middle East*, June 2015, 16-18.

Memiş, M. Ü. & Tüm, K. (2011). Sürekli denetim süreci ve iç denetim ile ilişkisi. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 37, 145-162.

Mengi, B. T. (2012). Hile denetiminde yetkinliklerin değerlendirilmesi – hile karosu. *Mali Çözüm Dergisi, 114*, 113-128.

Musa, H. (2017). The risk of fraud and the role of internal audit. *Internal Auditor-Middle East*, March 2017, 30-33.

O'reilly, A. (2006). Continuous auditing: Wave of the future?. *Corporate Board,* 27(160), 24-26.

Önce, S. & İşgüden, B. (2012). İç denetim faaliyetinin gelişen ve değişen bilgi teknolojileri ortamı açısından değerlendirilmesi: IMKB–100 örneği, *Yönetim ve Ekonomi Araştırmaları Dergisi,* 17, 38-70.

Özbek, Ç. (2012). *İç Denetim, Kurumsal Yönetim, Risk Yönetimi, Iç Kontrol*. İstanbul: Türkiye İç Denetim Enstitüsü Yayınları.

Prıcewaterhousecoopers (PWC) (2012). *Internal audit 2012 – asia pasific supplement*. Hong Kong. Retrieved from https://www.pwc.com/sg/en/advisory/assets/publication-internal-audit-2012asiapac.pdf

Rahman, R. A. & Anwar, I. S. K. (2014). Effectiveness of fraud prevention and detection techniques in malaysian islamic banks. *Procedia-Social and Behavioral Sciences,* 145, 97-102.

Ramamoorti, S. & Dupree, J. (2010). Continuous controls monitoring can help defer fraud. *Financial Executive,* 26(2), 66-67.

Rezaee, Z., Sharbatoghlıe, A., Elam, R. & Mcmickle, P. L. (2002). Continuous auditing: building automated auditing capability. *Auditing: A Journal of Practice and Theory,* 21(1), 147-163.

Searcy, D. L., Woodroof, J. B. & Colson, R. H. (2003). Continuous auditing: leveraging technology. *CPA Journal,* 73(5), 46-48.

Tang, F., Norman, C. S. & Vendrzyk, V. P. (2017). Exploring perceptions of data analytics in the internal audit function. *Behaviour & Information Technology,* 36(11), 1125-1136.

Teeter, R. A., Alles, M. G. & Vasarhelyi, M. A. (2010). The remote audit: a research framework. *Journal of Emerging Technologies in Accounting,* 7(1), 73-88.

The Chartered Instıtute of Management Accountants (CIMA) (2009). *Fraud risk management a guide to good practice.* London. Retrieved from https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

The Institute of Internal Auditors, The American Institute of Certified public accountants and Association of Certified Fraud Examiners (IIA-AICPA-ACFE) (2008). *Managing the Business Risk of Fraud: A Practical Guide***.** Florida. Retrieved from https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf

The Instıtute of Internal Audıtors. (IIA) ((2009). *Internal Auditing and Fraud*. Florida.

The Instıtute of Internal Audıtors. (IIA) (2011). *Global Technology Audit Guide (GTAG) 16: Data Analysis Technologies*. Florida.

The Instıtute of Internal Audıtors. (IIA) (2015). *Global Technology Audit Guide (GTAG) 3: Continuous Auditing: Coordinating Continuous Auditing And Monitoring To Provide Continuous Assurance*. Florida.

The Instıtute of Internal Audıtors. (IIA) (2016). *International Standards For The Professional Practice of Internal Auditing-Standards*. Florida.

The Instıtute of Internal Audıtors (IIA). (2019). *Fraud and internal audit – assurance over fraud controls fundamental to success. IIA Position Paper*. Florida. Retrieved from https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Fraud-and-Internal-Audit.pdf

Halkbank (HB). (2009). *2008 annual report*. Ankara. Retrieved from https://www.halkbank.com.tr/images/channels/English/investor_relations/financial_info/Annual_reports/halkbank2008_1.pdf

Halkbank (HB). (2016). *2015 annual report*. İstanbul. Retrieved from https://www.halkbank.com.tr/images/channels/English/investor_relations/financial_info/Annual_reports/2015_annual_report.pdf

The Institute of Internal Audit – Turkey (TİDE) (2016). *Sawyer's Iç Denetçiler Için Rehber, Cilt 2: Iç Denetim Süreçleri ve Yöntemleri*. İstanbul.

İşbank (İB) (2016). *2015 annual report*. İstanbul. Retrieved from https://www.isbank.com.tr/EN/about-isbank/investor-relations/publications-and-results/annual-reports/Documents/Isbank_2015.pdf

Vakıfbank (VB) (2016). *2015 annual report*. İstanbul. Retrieved from https://www.vakifbank.com.tr/documents/finansal/Annual_Report_2015.pdf

Uzun, A. K. (2002). Muhaberat teftişinden e-posta denetimine. *TİDE İç Denetim Dergisi,* 5, 37-38.

Uzun, A. K. (2009). Şirketlerde iç kontrollerin yeterliliğinde iç denetimin rolü. *Active Bankacılık ve Finans Dergisi,* 62, 1-8.

Vona, L. W. (2008). *Fraud Risk Assessment: Building A Fraud Audit Program*. New Jersey: John Wiley & Sons.

Ziraat Bank (ZB). (2008). *2007 annual report*. Ankara. Retrieved from https://www.ziraatbank.com.tr/en/Investor-Relations-ZB/Financials/Documents/AnnualReport2007.pdf

Ziraat Bank (ZB). (2016). *2015 annual report.* Ankara. Retrieved from https://www.ziraatbank.com.tr/en/Investor-Relations-ZB/Financials/Documents/AnnualReport2015.pdf