TİDE Academia Research
Sayı 3 / 55-82 (2021)

Case Study/Vaka Çalışması

USING BIG DATA IN INTERNAL FRAUD DETECTION

Teoman Samet TEMUÇİN[1]
Sefa ERBAŞ[2]
Anıl AY[3]

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 threating 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. *TİDE AcademIA Research*, 3(1), 55-84

Keywords: Internal fraud, Fraud detection, Big data

JEL Classification: C55, C8, K42, M42

TİDE Academia Research
Sayı 3 / 55-82 (2021)

İÇ SUİİSTİMALİN TESPİTİNDE BÜYÜK VERİNİN KULLANILMASI

Öz

İç suiistimaller, kurumları tehdit eden en önemli operasyonel risklerden biridir. Verdikleri büyük operasyonel kayıplara ek olarak, kurumların itibar ve prestij kaybına da neden olmaktadırlar. 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.

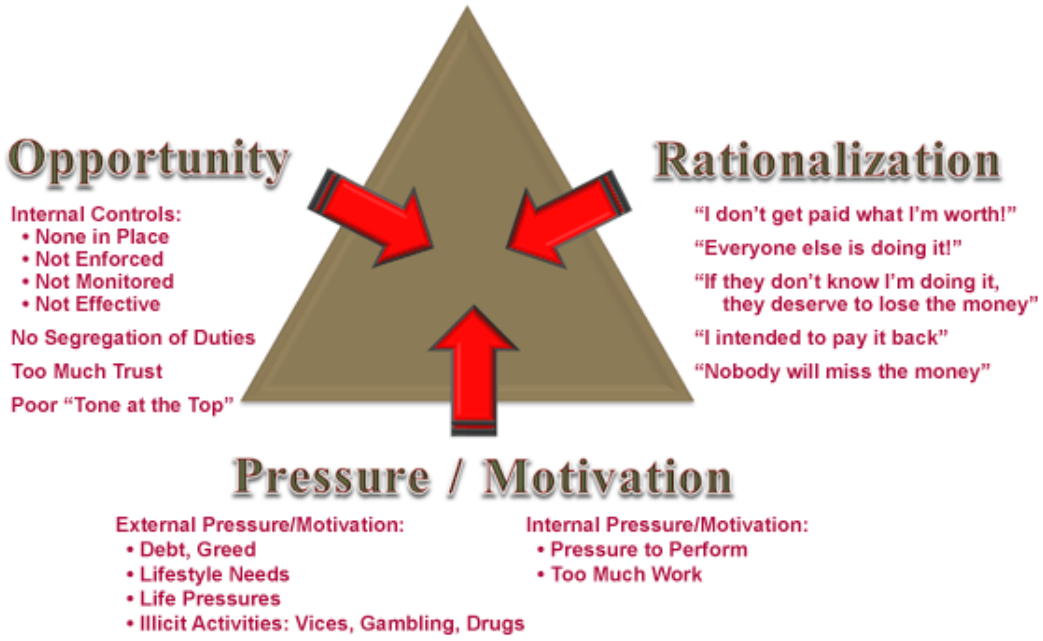

Figure 1: The Fraud Triangle

Source: Association of Government Accountants (n.d.)

The presence of these factors causes fraud attempts by the personnel. Wolfe and Hermanson (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 Bank[4] 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.

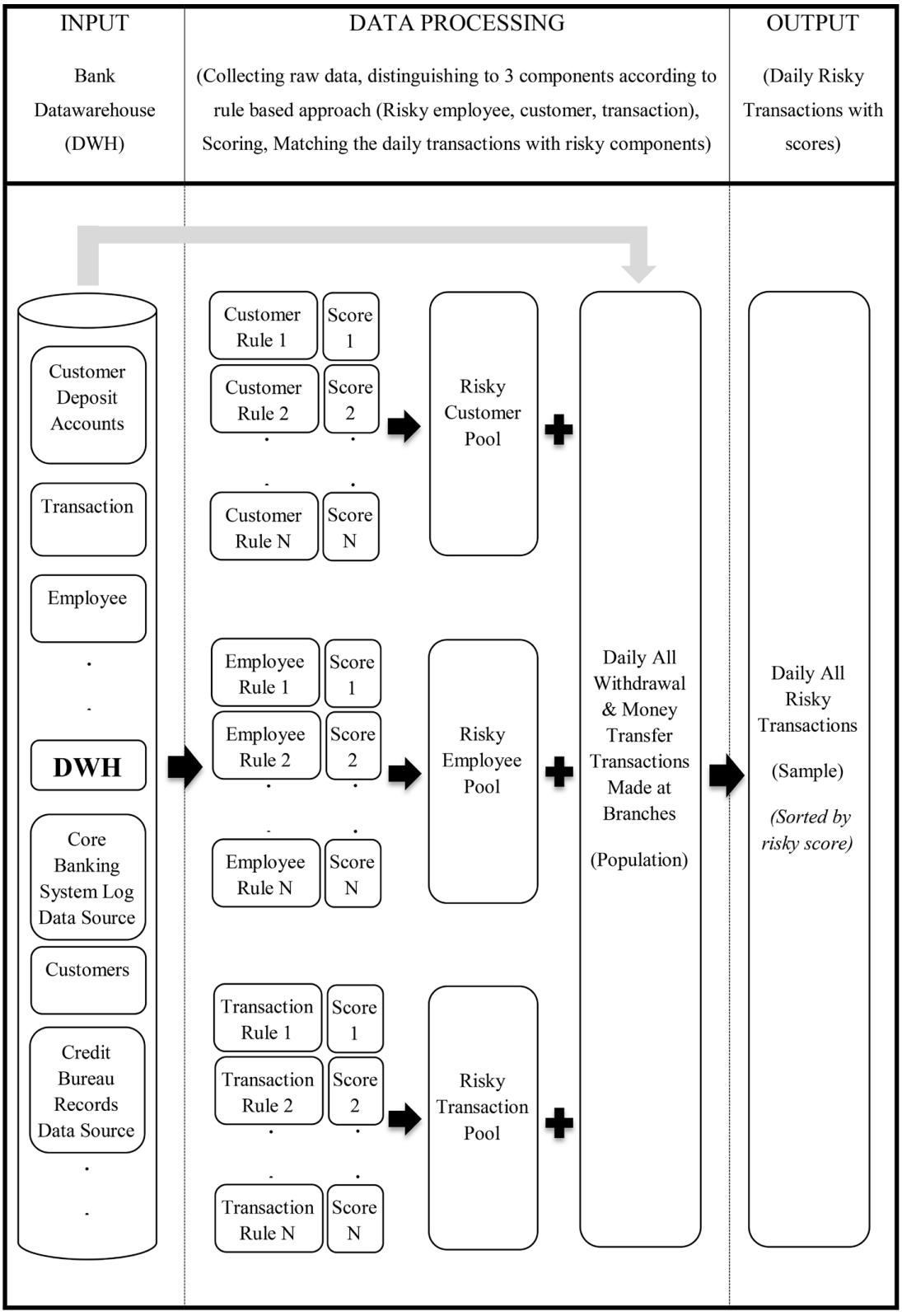

Figure 2: System Working Principle

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.