MIDDLE EAST TECHNICAL UNIVERSITY Ankara, Turkey

INSTITUTE OF APPLIED MATHEMATICS
http://iam.metu.edu.tr

In the Context of Control, Approach to the Risks Posed by Covid-19 in the Field of Banking within the COSO Internal Control-Integrated Framework

D. Genç

Abstract. Control are the measures taken by the management and other relevant units to manage risks and increase the likelihood of achieving the determined goals and objectives. These control processes are generally determined by certain frameworks and one of the most valid frameworks is COSO. Along with the pandemic, the risks that banks may face have partially changed. Therefore, control processes should change against these risks. In this study, it has been shown which COSO component these risks belong to and that there should be a dynamic control process with changing risks.

Keywords. Control, COSO Internal Control-Integrated Framework, COVİD-19, Banking Sector

Term Project

Student : Derya Genç
Advisor : Prof. Dr. Ömür Uğur

IN THE CONTEXT OF CONTROL, APPROACH TO THE RISKS POSED BY COVID-19 IN THE FIELD OF BANKING WITHIN THE COSO INTERNAL CONTROL-INTEGRATED FRAMEWORK

A TERM PROJECT SUBMITTED TO

THE GRADUATE SCHOOL OF APPLIED MATHEMATICS

OF

MIDDLE EAST TECHNICAL UNIVERSITY

BY

DERYA GENÇ

IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS

FOR

THE DEGREE OF MASTER OF SCIENCE

IN

FINANCIAL MATHEMATICS

JANUARY 2023

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

NAME SURNAME: DERYA GENÇ

Signature: .....

Acknowledgement

I would like to express my special thanks of gratitude to my supervisor Prof. Dr. Ömür Uğur for providing his comments, suggestions and encouragement throughout the project.

Abstract

Control are the measures taken by the management and other relevant units to manage risks and increase the likelihood of achieving the determined goals and objectives. These control processes are generally determined by certain frameworks and one of the most valid frameworks is COSO. Along with the pandemic, the risks that banks may face have partially changed. Therefore, control processes should change against these risks. In this study, it has been shown which COSO component these risks belong to and how control processes develop. Moreover, it is understood that there should be a dynamic control process with changing risks.

Keywords

Control, COSO Internal Control-Integrated Framework, COVİD-19, Banking Sector

Contents

Chapter 1

Introduction

Internal control is a process designed to provide reasonable assurance. It is carried out by the board of directors, management and other employees of the enterprises. Reasonable assurance is given by internal control about the reliability, accuracy and compliance of applicable laws/policies/procedures of the information obtained and financial reports. Internal controls aims to identify risks/problems, take corrective actions, and prevent mistakes/irregularities. Guidelines allow organizations to consider all aspects of internal control. It is published by various professional organizations. It is not mandatory in most countries. However, if implemented, it provides reliability to companies in terms of corporate governance. In our country, the regulation on systems was put into force by BDDK. The regulation has been prepared on the basis of the COSO internal control model (Madendere, 2005).

Commission (COSO) was formed in 1992 when some organizations came together to evaluate internal controls. The Covid-19 crisis has shown its effect in almost every sector. Radical measures of the actions is taken due to the pandemic. In addition to the measures taken to protect human health, necessary precautionary packages have been created for the strong survival of the economies. The paper by Sertkaya says that countries with strong economies are more likely to endure the economic burdens brought by the epidemic while countries with weak and fragile economies suffered more (Sertkaya, 2021). In this study, some of risks have been examined and how it has changed in the banking sector or whether there is a risk in the banking sector is examined by using other studies in the literature. With Covid-19, new risks have emerged as well as existing risks, such as cyber risks, fraud risks, reputation risks, supply chain risks, health and safety risks (KPMG, 2020a). In Chapter 5, we see what risks we deal with. Shortly, with the pandemic, the use of technology and innovative developments in the field of

banking have increased. With the increase of digitalization, cyber crimes are increasing and cyber security systems are becoming more important. Also, in Turkey, as in other countries, it has rearranged its working activities to protect both customers and employees from COVID-19. They have established the necessary infrastructure systems in order to work remotely and be accessible. With the pandemic, new/changing risks have entered our lives and the existing control mechanism may be missing. Therefore, measures should be taken against the risks encountered, regulations should be made, and control mechanisms should be reviewed. In our study, it has been examined which title of COSO, which presents the framework of the control mechanism with these changes, reveals a situation related to it. The conclusion chapter comments on our results and possible future work.

Chapter 2

Turkish Banking Industry

Banks have an important place in financial markets. Banks collect funds from those who have surplus and give them as loans to those who demand funds. One of the most important tasks of banks is to ensure the exchange between savings and investments. In addition to the flow of funds, it also has important duties in economics such as creating fiat money and helping to implement monetary and fiscal policies. For this reason, the country's economy and the banking sector are intertwined elements. According to June 2022 data published in the BDDK (Banking Regulation and Supervision Agency) in Turkey there is:

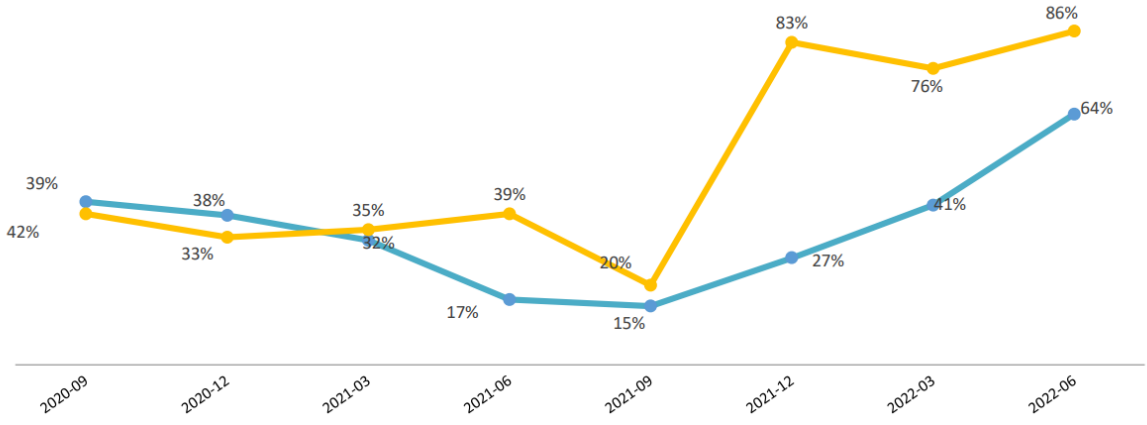
-A total of 57 banks which are 13 public, 16 local private and 28 foreign according to ownership,

-35 deposit, 6 participation and 16 development and investment banks,

-The total number of personnel increased by 1.040 compared to the previous quarter and reached 202,637 persons,

-The total number of branches in the banking sector reached 11,091.

Total Asset Annual Growth Rates(%) are given below (BDDK, 2022):



Blue- Turkish Liras- Growth Rate, Yellow- Foreign Currencies-Growth Rate

2.1 Measures Taken for the Turkish Banking Sector Against the COVİD-19 Crisis

During the pandemic period, some regulations were introduced to prevent negative changes in banks' balance sheets. Banking Regulation and Supervision Agency (BDDK) and the Central Bank of the Republic of Turkey introduced the regulations in the banking sector aimed to ensure that the economy is affected at a minimum level.

Some of these regulations/measures are as follows (T.C. İstanbul Valiliği, 2020):

-Delaying loan principal and interest payments to companies in need for at least 3 months,

-Increasing the Credit Guarantee Fund (KGF) limit from 25 billion lira to 50 billion liras,

-Increasing the loanable amount from 80 percent to 90 percent in houses under 500 thousand liras,

-Enabling flexible and remote working models,

-Providing short-time working allowance in workplaces that have suspended their activities.

Chapter 3

Effects of COVİD-19 Pandemic on Turkish Banking Industry

The Coronavirus was first seen in Wuhan, China in December 2019, and then rapidly spread across the country. It has negatively affected all economies. The crisis experienced is not only an economic/financial crisis, but also a health crisis.

During the pandemic period, Turkey was experiencing problems arising from both internal and external dynamics. For some reason, economic difficulties were expected in 2020 even before the pandemic. For example, US-China global trade wars, Brexit process, FED's change in interest rates and geopolitical instabilities. With the addition of the Covid-19 outbreak, the estimates were revised downwards again. The Turkish economy was directly affected by these developments (Sertkaya, 2021).

Every country such as Turkey that wants to reduce the effects of the pandemic/increase the measures had to take action. During the pandemic process, domestic/international travels were prohibited, workplaces were closed and a curfew was declared. Such measures have brought some industries to a standstill. Mainly flights, transportation, sports, education, trade and service organizations were also affected by the pandemic (Duran, 2020).

Pandemic caused an increase of unemployment and inflation rate. At the same time, the deterioration of the budget and balance of payments due to the pandemic, the growth rate and external financing difficulties have been experienced. The measures implemented during the pandemic process had a negative impact on the economy, causing a global crisis. For this reason, countries have tried to take precautions by taking some policy decisions and measures (Arabacı, 2020).

The financial sector in Turkey has a bank-dominated structure. For this reason, banks have played an important role in transferring the measures taken with the pandemic to the market. The real sector has been tried to be supported by the banks with additional precautionary packages, for example; reserve requirement lowering the interest rates, non-performing loans such as the extension of delay times (Dağıdır Çakan, 2021).

With the credit policy implemented in Turkey within the scope of the COVID-19 pandemic, special credit packages and credit channels were kept open. Accordingly, loan volume of TL 2.6 billion at the end of 2019 with active implementation of the ratio (It is between the deposits that banks collect and the loans, securities and swap transactions that they use for this resource) reached 3.1 billion TL in April 2020. At the end of October, it reached its highest level with 3.7 billion TL. Thus, the credit volume increased by 35% in one year and reached 3.6 billion TL at the end of 2020. While state-owned banks stand out in the increase in loans, foreign capital banks maintained their current status (Kocaman, 2021).

The financing need created by the COVID-19 pandemic has been met by banks to a significant extent. This situation allowed deposit banks to extend low-interest loans to the market during the pandemic period. Funding costs increased due to low-interest loans. Even interest income remained below interest expenses. Therefore, the net income from the interest was negative. As a result, the profits of especially state-owned deposit banks decreased. Since low-interest loans are funded with high-cost deposits, banks' net interest revenue rates have fallen (Kocaman, 2021).

As Beybur and Çetinkaya stated: Along with the pandemic, the banking sector has taken many measures to protect employees and customers. Digitally advanced banks have developed more in the digital field and turned the pandemic into an advantage. The measures taken by banks in the digital field are as follows:

-The joint ATM project, which started to be implemented in Turkey on October 1, 2009, allows the customer to perform a certain transaction using an ATM device of any bank. It is a system that allows transactions to be made in return for a fee. During the pandemic period, some of

the banks have enabled the use of shared ATMs free of charge. Like this, customers to avoid contact as much as possible and get faster service has provided.

-Applications for consumer loan were made by internet banking and mobile banking channels in order to avoid intense contact.

-In order to prevent customers from contacting POS devices that are used by everyone, the password requirement has been removed for transactions with a certain amount.

-The banking sector is a structure that requires contact with customers. However, during the pandemic period, employees with chronic illness or Covid-19 were allowed to work from home in order not to be affected by the epidemic. Thus, they aimed to protect both the customer and the employee.

-During the pandemic period, transactions and limits that can be made from ATM devices have been increased.

-During the pandemic period, banking transactions such as EFT and money transfer provided no fee. Thus, it was aimed to reduce customers' contact with the bank.

TBB says about the number of active digital banking customers in Turkey:

Number(thousands)/Time Interval	July-September 2021	April-June 2022	July-September 2022
Number of active digital customers	73,440	85,130	90,579
Corporate	3,110	3,796	3,862
Individual	70,330	81,335	86,717

Source: Compiled from TBB Digital, Internet and Mobile Banking statistics. (TBB, 2022)

As can be understood from the data received from the TBB, the guidance made in the field of digital banking during the pandemic period has worked and the digital bank channel has increased in both individual and corporate areas. Thus, customers chose the digital channel instead of the branch channel, protecting both themselves and the employee.

TBB says about the number of ATMs, employees, POS in banking sector in Turkey:

Number/Time Interval	2019	2020	2021
Number of ATMs	46,998	46,886	46,501
Number of Employees	188,837	186,612	185,248
Number of POS	2,911,909	3,364,699	4,253,501

Source: Compiled from TBB Digital, Internet and Mobile Banking Statistics. (TBB, 2022)

When the table is examined, it is seen that although the use of digital channels has increased, the number of employees has decreased, but the use of POS, where contactless payments can be received from customers, has increased. As it can be understood, the measures taken in the field of banking during the pandemic period have worked, and the tendency towards digital channels and contactless payment channels has increased. There have been significant changes in Turkish banking in terms of employees and customers with the pandemic, and the main interaction areas are given below. The reflection of the epidemic on banks has been on both customers and employees. In this process, banks created measures and financial resources for their customers, and also created precautionary items for their own employees to protect against the epidemic. Banks have postponed the loan payments of companies or individuals whose cash flow has deteriorated, restructuring and loan support packages for these companies or individuals. Banks have taken a series of measures regarding hygiene rules, working hours and working styles to protect the health of its employees.

In the banking system, different loan support packages have been created by some banks, such as holiday support loans, advantageous housing loans, vehicle loans. Government policy decisions were taken to minimize the negative effects faced by customers. With these decisions, various economic and financial supports such as deferring tax and credit debts, providing liquidity and aid packages to KOBİ were provided to companies. The global epidemic has led to many innovations in the banking sector, as well as enabling new changes and transformations. Banks also have allowed employees to work from home to protect both customers and employees during the pandemic. In order to protect the health of branch employees and customers in contact with customers, plexiglass separators were placed in the branches. All branches and buildings were disinfected. Masks, disinfectants, gloves, etc. were provided to all employees working from work locations. Hygiene protective products continue to be provided uninterruptedly. In addition to all these, work continues uninterruptedly to make working environments healthier (GarantiBBVA, 2023).

The banking sector was one of the sectors that took measures very quickly from the moment the coronavirus epidemic began to appear in Turkey. Banks promptly directed their head office

employees to work from home, while at the branches they started to work in turns and to work remotely. Meetings have been moved to the digital environment (Hürriyet, 2020).

Although most transactions are directed to mobile channels, customers may need to come to the branch for some transactions, especially older customers may choose branch channels because their mobile usage is lower. In this case, banks have taken some measures to protect customers and employees, such as the use of thermometers, the use of gloves, the creation of social distance areas. Actions were taken not only at the branches, but also at the headquarters and regional directorates. Table layouts were reconstructed and distance was maintained. In addition, posters for disease prevention and hygiene recommended by the Ministry of Health were kept.

At the same time, rules were announced for branches with the guide titled "Prevention and Control Measures in Bank Branches" prepared by the Ministry of Health, taking into account the recommendations of the Coronavirus Scientific Committee in Turkey.

In this context, it has been made mandatory for employees to wear medical masks. Care has been taken to ensure that the numerators in the branches are used by only one person, and that they must be regularly disinfected. Care was taken to ensure hand hygiene by keeping alcohol-containing hand antiseptics at accessible points in order to prevent the spread of the epidemic (T.C. Sağlık Bakanlığı, 2020). Also, The Banks Association of Turkey (TBB) recommended the new working hours to banks between 12.00 and 17.00. Some banks implemented this decision, while some banks continued their old working systems by taking the necessary precautions.

With COVID-19, the importance of efficient, uninterrupted business activities and risk management has been understood more clearly. It is a necessity for every institution to make risk management healthy. It is the responsibility of senior management to establish a risk management framework on behalf of the board. Control responsibility, on the other hand, is a phenomenon that belongs to every employee. Risk management and control are related concepts. After this section, information about the control and control framework is given, and an approach to changing/emerging risks is given on the basis of control framework.

Chapter 4

What is Internal Control?

Internal control is a process designed to provide reasonable assurance. It is carried out by the board of directors, management and other employees of the enterprises.

Reasonable assurance is given by internal control about the reliability, accuracy and compliance of applicable laws/policies/procedures of the information obtained and financial reports. Internal controls aims to identify risks/problems, take corrective actions, and prevent mistakes/irregularities. In summary; control has some key points:

-Internal control is a process.

-It is the tool used to achieve the goals of the business, not the goal.

-Internal control is people at all levels of the organization, not just guidelines and form.

-The assurance provided by internal control to management and the board of directors is reasonable assurance, not absolute assurance.

The main purpose of establishing internal controls to further strengthen businesses;

-Reliability and integrity of information,

-Compliance with policies, procedures, laws and regulations,

-Protection of assets,

-Efficient use of resources,

-Realization of business goals and objectives (Audit & Advisory Services).

4.1 The Types of Internal Control

Classification of internal controls; preventive controls, detective controls, directive controls and corrective controls below explained under the subheadings (Melikyan, 2015).

Different risks require different types of controls. A combination of these controls can also be used against the risks that have occurred or will occur.

1. Preventive Controls: It aims to secure the operation of the systems. It ensures that undesirable situations do not occur. For example, competent staff recruitment, ethical codes, segregation of duties and good control environment can be given. In addition, measures such as locks, passwords and security personnel are also included in such controls (Melikyan, 2015).

2. Detective Controls: Detective controls, which are more costly than preventive controls, can be used to measure preventive controls effectiveness. It is not possible to predict all possible errors. The controls that enable these realized errors to be revealed are called detective controls such as process/product controls, alarm etc (Melikyan, 2015).

3. Directive Controls: It provides guidance on the achievement of goals. To motivate people and lead them to a goal are positive applications. They promote the occurrence of a desired state such as ethical codes, legislation, personnel training on a specific subject, emergency case procedures (Melikyan, 2015).

4. Corrective Controls: Controls that are intended to compensate for controls that do not exist or that may be too costly. Sometimes there are insufficient financial or human resources to implement preventive controls. For example, there may not be enough staff for the implementation of the principle of segregation of duties. Corrective controls are usually performed post-processing. They are shorter-term and narrow-scoped controls than detective controls. Hotlines and applications which have a detective and preventive nature, it essentially has a gap-filling structure (Melikyan, 2015).

4.2 The Control Frameworks

Guidelines that allow organizations to consider all aspects of internal control. It is published by various professional organizations. It is not mandatory in most countries. However, if implemented, it provides reliability to companies in terms of corporate governance. Below are some of the control frameworks published in the field of internal control:

-COSO Internal Control Model developed in the USA (Committee Of Sponsoring Organizations)

-CoCo Internal Control Model in Canada (Criteria Of Control),

-Turnbull Report in the UK,

-King Report in South Africa,

-Vienot Report in France.

Apart from these controls, there are other frameworks such as COBIT, SAC, SAS55, SAS78, SysTrust (Uzunay, 2007).

In order to increase the transparency and efficiency of the enterprises, the control requirements on the fields of activity are increasing day by day. In this respect, many different internal control system models have been developed and revised at the international level. The COSO model developed in the USA and the COCO model developed in Canada are two models that are widely used around the world (Bakkal et al, 2012). The regulation on internal audit and risk management of banks systems in our country was put into force by BDDK. The regulation has been prepared on the basis of the COSO internal control model (Madendere, 2005). Banks need effective structures and competence to achieve their goals. On the other hand, they have to make the best of strong governance and risk management. The management, operating results, etc. related to the bank are reported to the governance. Governance relies on internal audit for independent, objective assurance, offering advice and promoting innovation.

The triple line model defines the structures and processes that help banks achieve the goals they set, provide strong governance and manage risk. This model can also be applied to other non-bank institutions. Management has a responsibility to achieve goals. Achieving these goals encompasses both the 1st and 2nd line roles. First-line roles are generally responsible for delivering products and services to bank customers. The purpose of second line roles is generally risk management in certain areas such as information, technology security, sustainability and quality assurance, compliance, internal control. 3rd line roles include internal auditing (IIA, n.d.). Prior study from Al-Shetwi (2011) says that for the effectiveness of corporate governance, internal audit is important. Also, according to Gay and Simnett (2007), the internal audit is necessary to create security for fraudulent use of assets in banks. It is also necessary to rely on reports such as financial statements. Therefore, the governance quality is directly about the internal audit quality. In order for internal audit to be reliable and independent, it must be kept separate from the governing bodies.

4.3 COSO Internal Control- Integrated Framework

The Committee of Sponsoring Organizations (COSO) was formed in 1992 when some organizations came together to evaluate internal controls. These organizations are given below (Aksoy, 2005):

- AAA- American Accounting Association,
- AICPA- American Institute of Certified Public Accountants,
- FEI- Financial Executives Institute,
- IIA- Institute of Internal Auditors,
- IMA- Institute of Management.

These organizations have developed a model called “Internal Control-Integrated Framework” and this model has been adopted as the generally accepted framework for internal control (Aksoy & Aksoy, 2020).

In fact, risks are inherent in both risk management and internal control. It is not possible to talk about internal control or risk management without risk. Therefore, internal control and risk management are inseparable. Thus, by making inferences from COSO Internal Control-Integrated Framework model, an enterprise risk management framework was created. Thus, the COSO framework has become one of the most widely used resources in internal control and enterprise risk management processes (Karakaya, 2019, s. 21). The COSO ERM Framework began to develop around 2000 and was published in 2004 under the name of “Enterprise Risk Management-Integrated Framework” in which the corporate risk dimension was defined. COSO has been developed to follow current developments such as globalization, technological breakthroughs, digitalization and diversification of fraud risks and has been updated from time to time. The COSO 2004 framework was updated in 2017. The current risk management framework has been published by COSO under the title of “Enterprise Risk Management – Aligning Risk with Strategy and Performance”. The basic risk assessment principles defined by

COSO are as follows:

-Determination of Goals: Every business has goals. The risks to be encountered while reaching these targets should be known and the effects of exposure to risk should be revealed.

-Identification and Evaluation of Risks: It is necessary to identify and examine the risks that will affect the achievement of the objectives in terms of management. Relationship of risks with each other, risk analysis should be done.

-Evaluation of Fraud Risks: The fraud risks that companies may be exposed to while reaching their targets should also be considered.

-Responding to Risks: After identifying the risks to be exposed, how to respond to the risks should be evaluated (Türedi & Koban, 2016).

As it is known, institutions are units that want to achieve operational, compliance and reporting targets. In 2013, the COSO - Internal Control-Integrated Framework was also updated. The 2013 Framework is a flexible, reliable, up-to-date and cost-effective framework for the design and evaluation of internal control systems for organizations seeking to achieve these goals (Sobel et al., 2019). The 2013 Framework is applicable to all businesses, regardless of organization size or type, such as public companies, private companies, nonprofits, and government agencies.

Briefly, the COSO internal control model provides the framework for the structure necessary for the successful advancement of activities in businesses. It is a structure developed for the actions to be taken against the risks that companies face or will encounter, and for the continuity/updateness of the processes (Türedi, 2014).

COSO Internal Control-Integrated Framework Components and Principles:

Management's perspective on internal control systems is an important factor for effective control. If management attaches importance to internal control systems and emphasizes this situation, employees will also attach more importance to controls. When employees feel that internal control is disregarded by management, there is little chance that control objectives will be achieved (Rezaee, 1995). Commission (COSO) was formed in 1992 when some organizations came together to evaluate internal controls. COSO Framework components;

Control environment: It defines the standards, processes, and structures required for the execution of internal control throughout the organization.

It expresses the working environment of the institution and forms the basis of the internal control system. It contains abstract and subjective elements. It relies on soft controls, which is difficult to define in a specific way such as corporate culture, leadership, morale, honesty, openness. The control environment is created with hard controls, which can be clearly defined such as organizational structure and corporate policies. Examples of an unhealthy control environment are bribery by senior management, assignment of incompetent employees, and lack of written codes of ethics.

Risk assessment: Risk is defined as the probability that an event will occur and adversely affect the achievement of organizational goals. Risk assessment is the basis for determining how to manage these risks. That is; evaluation of risks is the prioritization of risks by evaluating their impact and probability. Risk assessment helps determine the most appropriate response in terms of benefit/cost balance. During the risk assessment phase, answers are sought for the following questions:

-What are the goals?

-What are the available controls?

-What are the possible consequences if the risk materializes?

-Will the activities of another unit/organization affect my risk?

-Who are the stakeholders? What is their level of experience and expertise?

Control activities: Actions that help businesses reduce risks to achieve their goals. Control activities can be preventive or detective. It can also be carried out at all levels of the business. That is; control activities are policies and procedures applied to facilitate the achievement of operational objectives by reducing the impact or probability of a risk. Cost-benefit analysis should be done before putting control activities into operation. Examples of control activities: Separation of duties, authorization, reconciliation, performance review, physical controls, IT controls.

Information: It is obtained or produced from both internal and external sources. They support internal controls. **Communication:** It is used to disseminate necessary information inside and outside the organization, based on internal and external sources. Communicating information covers all relevant, quality, internal and external information. Accurate information must be communicated to the appropriate people in a timely manner. The objectives, targets, activities and results of the institution should be reported to the relevant parties. Institutions should have an appropriate information and communication system in order to monitor the performance of the units and employees, and to ensure that the decision-making processes can operate in a healthy way. For example; establishing methods for reporting errors, irregularities and corruption.

Monitoring activities: This process is the stage where it is observed whether the control system is progressing in a healthy way. It is intended to evaluate the quality of performance. For examle; monitoring whether or not risk assessment works as desired.

Here are 17 principles mapped to the five components defined in the COSO Framework (COSO, 2019).

Exhibit 2. **5 components and 17 principles of internal control**

5 components	17 principles
Control environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability.
Risk assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys control activities through policies and procedures
Information and communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Source: Adapted from the COSO "Internal Control – Integrated Framework"

The control systems applied before the pandemic may be insufficient to manage the risks that come/change with the pandemic. Inadequate control systems, on the other hand, can pose a threat to sustainability for institutions. Therefore, the control system needs to be updated based on a control framework. The COSO Integrated Internal Control Framework provides guidance in terms of renewing and updating control systems according to changes in business and activity areas, and increases the effectiveness of the role of internal control in achieving targets.

Chapter 5

Evaluation of Risks Arising/Changing with the Pandemic in the Field of Banking

With the emergence of COVID-19, the importance of "predicting the unpredictable: dealing with risk and uncertainty" has gained value.

The Covid-19 crisis has shown its effect in almost every sector. Radical measures of the actions taken due to the pandemic we see that. In addition to the measures taken to protect human health, necessary precautionary packages have been created for the strong survival of the economies. Countries with strong economies are more likely to endure the economic burdens brought by the epidemic while countries with weak and fragile economies suffered more (Sertkaya, 2021).

With Covid-19, new risks have emerged as well as existing risks, such as cyber risks, fraud risks, reputation risks, supply chain risks, health and safety risks (KPMG, 2020). KPMG shows the new and changing risks that have entered our lives with COVID-19. According to it; the risks are fraud, cyber, risk/compliance culture, new regulatory requirements/opportunities, physical/mental health/safety, contract obligations, virtual workplace, reputation, business continuity/crisis management/emergency plans, disruption and innovation, economic downturn, working capital/cash management (incl. credit risk)/insurance, social/political instability, transport/logistic/travel, strategy/financial plan, steering information/data, stakeholder management/communication, tax/trade, third party management/supply chain.

With the pandemic, banks started to take measures one after another. Some measures/actions have been taken against the pandemic with the guidance of authorities, bank headquarters and international institutions. For example; many steps have been taken in areas such as bank working hours, working systems, infrastructure systems, health-hygiene practices. In addition, referrals to digital channels have increased and the importance of using more secure systems

has been understood. In summary, it has experienced action/target/policy changes to adapt to changing environmental conditions. Therefore, some risks faced due to the steps taken in changing conditions have changed. With the introduction of Covid-19 into our lives, there have been important developments in the banking sector. Steps have been taken to adapt to the emerging pandemic environment; directing customers to digital channels, working remotely. We see above that digital customers have increased with pandemic.

In this study, the changing structure was examined in order to adapt to the changing environment in the field of banking. Along with this changing structure, some of the changing risks in banking have been examined. Control activities required for risk management in institutions are explained and their necessity is mentioned. The risks that have arisen/changed with the effect of the pandemic in the banking sector have been approached within the framework of the COSO Internal Control-Integrated Framework. COSO mentioned that there should be 5 basic components to ensure the necessary effectiveness in internal control. The question of how to approach the changing risks in order to increase the control efficiency is given under the relevant headings of the 5 components.

As mentioned above, the use of digital channels has increased even more with the guidance made in the digital field in the banking sector. New regulations have come, infrastructures have been created, and customer use has increased. Therefore, with the increase in digitalization, a new/changing environment has emerged for the risks that may arise in banking transactions. Some risks that may be encountered in the digital are described below.

Cyber Risk

With Covid-19, new risks have emerged as well as existing risks, such as cyber risks, fraud risks, reputation risks, supply chain risks, health and safety risks (KPMG, 2020).Cyber risk can be defined as the risk of loss arising from the digital environment (Curti et al., 2021). For example; Yahoo Cyber Attack: Yahoo is a digital portal with services such as search engine and e-mail. Towards the end of 2014, Yahoo was hacked and as a result, the accounts of more than 500 million people were hacked. In a statement after this development, the company confirmed

that credit card information is safe, but users' basic information and passwords were stolen (Volz, 2016).

With the pandemic, the use of technology and innovative developments in the field of banking have increased. With the increase of digitalization, cyber crimes are increasing and cyber security systems are becoming more important. In the banking sector, daily withdrawal limits at ATMs have been increased as customers can not enter branches due to the pandemic. In this challenging process, banks have made many transactions possible through mobile channels in order to direct customers to digital channels (www.akbank.com.tr). However, with the sudden emergence of the pandemic, some businesses were caught off guard. There may be businesses that have to take quick action to respond to customer needs, although they do not have enough technology and employees that can cause security weakness. As a result, cyber risk has increased more than other sectors, especially in the financial sector due to the pandemic (Aldasoro, 2021). With the pandemic, companies' digital transformation has accelerated and cyber security has now become a major concern. Ignoring cybersecurity risks can have significant reputational, operational, legal and compliance implications. According to the information received from the NCSC (National Center for Cyber Security) in June 2020, 350 cases of cyber attacks (phishing, fraudulent websites, direct attacks on aircraft, etc.) took place in Switzerland in April, compared to the norm of 100-150 (Deloitte, 2021). Some type of fraud can also be thought of as cybercrime.

The Association of Certified Fraud Examiners defines fraud as “any illegal acts characterized by deceit, concealment or violation of trust.” The main example of fraud is phishing scams. Scammers with phishing, tries to trick customers into obtaining their personal information. With the pandemic, more use of digital channels and remote working have become the new standard. Thus, the risk of fraud has also changed and new fraud scenarios have emerged. The validity and functionality of legacy controls became questionable. In short, with remote work and the use of digital channels, new opportunities for phishing theft have arisen (KPMG, 2020). According to KPMG; banks' workflows and processes have changed due to the pandemic, such as remote and flexible working hours. To avoid these risks, companies should control and

improve their cyber security, prefer a secure network for remote work, and inform their employees (KPMG, 2020b).

According to Deloitte; antivirus protection: Employees must be provided with an antivirus and anti-malware license. Cyber security information: Employees should be informed about cyber risks. Phishing protection: employees should be careful when receiving emails and check the authenticity of the sender's address. Network protection: employees should protect their Wi-Fi networks with a strong password and connect to networks they trust (Deloitte, 2021).

It is necessary to evaluate the new risks arising from the changes caused by COVID-19 and to implement the controls related to these risks quickly. In this case, existing controls should be re-evaluated and ensured that they work effectively (Sebilcioğlu, 2020).

When the measures to be taken against the increasing cyber risks with the pandemic are examined, it is mentioned that a safe network against cyber threats and personnel information are jointly mentioned. In the context of internal control, action should be taken regarding information and communication-control activities, which are among the 5 basic components according to COSO. It is important that banks/institutions adopt an agile/up-to-date control since events such as pandemics are not within the framework of certain periods such as annual or monthly.

When we make use of the COSO Framework: It has been understood that the following should be done in the control of these risks; using relevant information, communicating internally/externally, selecting and developing control activities- general activities over technology against cyber risk, deploying control activities through policies and procedures which should be updated with developments in cyber. Thus, it is given how to approach this risk, which has changed with the COSO Framework approach. It is important to implement these steps in order for the control processes to work more healthily.

Moreover, as mentioned above, with the pandemic, remote working has become the new standard. Therefore, with the increase of remote working, a new/changing environment has emerged for the risks that may arise in banking transactions. Some of the risks that may be encountered in this environment are described below.

Remote Working

In Turkey, as in other countries, it has rearranged its working activities to protect both customers and employees from COVID-19. They have established the necessary infrastructure systems in order to work remotely and be accessible. With the infrastructure created, most of bank employees work out of the office with remote access. Banks have decided to stop the travels of their employees, especially abroad, during the pandemic period. The recommendation to wear a mask published by the scientific board has been taken into account by the banks.

Bank branches have taken some precautions during the pandemic period, for example measures for bank security officers published by the Ministry of Health in 2020.

In the relevant security recommendations; in order to prevent face-to-face contact, they stand in a glass cabin, use masks and glasses/face protectors in close contact with the customer, and ensure hand hygiene constantly (T.C. Sağlık Bakanlığı, 2020).

With the pandemic, banks suddenly put the remote working process on the agenda and did not have much time to adapt.

The risk of division/concentration of the work has arisen for the employee who leaves the office environment with remote work, such as telephone / knocking on the door, the intervention of other people at home. Teamwork has become more difficult now that it is not face-to-face but in online environments. In such cases, the employee is likely to have difficulty maintaining concentration and discipline. In addition, being away from social life/isolation and the expectation of being reachable by the employer are other difficulties of working remotely at home (Erbuğ, 2019). According to Huremović, anxiety can be a symptom that occurs in quarantine and isolation situations. Employees are affected by dramatic changes in their lives, such as having to leave their social relationships. In this case, their anxiety may increase (Huremović, 2019). Therefore, bank employees who suddenly started to work remotely with the pandemic may face not only technological risks but also psychological risks. Mixing home-work life can increase anxiety levels. Due to psychological factors, the concentration of the personnel who are expected to serve within a certain period of time may decrease and may

cause errors in operations such as operational transactions. Additionally, the ergonomics of home furniture may not be optimal for working remotely for long periods of time. As a result, it can cause disorders in the musculoskeletal system. Namely; working home can cause both physical and psychological. The need to renew labor-worker's health and job safety-security procedures in the face of the new environment has arisen (ILO,2020).

The approaches of some authorities for such risks that have just entered / changed into our lives with the pandemic are given below. According to ILO (2020); employees should know how to contact technical support staff when they need help. Managers should be guiding, motivating and exemplary with their behavior. Moreover, new options such as access to hotlines, counseling, employee support programs, etc. should be created or existing options should be improved for employees to share their fears and concerns and labor-worker's health and job safety-security procedures should renew. According to T.C. Ministry of Family Labor and Social Services (2021); working in an unsuitable environment can cause ergonomic discomfort so necessary conditions should be provided at home to prevent it.

According to KPMG (2020); labor-worker's health and job safety-security procedures should be updated. Personal protective equipment should be provided for workers, procedures should be documented/updated, mental health programs, training and awareness should be increased.

It is necessary to evaluate the new risks arising from the changes caused by COVID-19 and to implement the controls related to these risks quickly. In this case, existing controls should be re-evaluated and ensured that they work effectively (Sebilcioğlu, 2020).

When the measures to be taken against the risks about working home with the pandemic are examined, it is understood that with the start of working at home, there may be a lack of equipment in the office. In addition, the stress level on employees can change with the sudden relocation of employees and starting to work at home. These situations can create both mental and physical problems on the employee. It is important to support employees in these areas. In terms of labor-worker's health and job safety-security , we went out of the office and the conditions were different. Therefore, up-to-date procedures should be established in line with changing conditions.

The COSO framework has informed us of the 5 components necessary for effective control, and when examined through this framework; the title of control activity describes the importance of company policies and procedures in terms of control. Therefore, policies and procedures established in response to changing conditions are associated with control activities according to the COSO Framework. In addition, one of the most basic conditions for the success of the internal control system is the existence of the control environment. It expresses the working environment of the institution and forms the basis of the internal control system. It contains abstract and subjective elements. That is; with pandemic, changing safety, physical and psychological conditions is about control environment of COSO components.

When we make use of the COSO Framework: It has been understood that the following should be done in the control of these risks; selecting and developing control activities, deploying control activities through policies and procedures which should be updated with developments about remote working, demonstrating commitment to integrity and ethical values, competence, enforcing accountability, establishing structure, authority and responsibility, namely, it is important to make the control environment healthy by creating a healthy work environment for the employees . Thus, it is given how to approach this risk, which has changed with the COSO framework approach. It is important to implement these steps in order for the control processes to work more healthily.

Chapter 6

Conclusion

In this study, some of the above risks have been examined and how it has changed in the banking sector or whether there is a risk in the banking sector is examined by using other studies in the literature. Then, it is given under which component these risks are evaluated in the COSO framework used in the control processes and an approach is given to how they should be evaluated according to the principles of the framework.

The banking sector is a structure that is intertwined with the national economy. Basically, the bank gives the surplus funds to people in need of funds. Therefore, banks play an important role in the country's economy. The pandemic has adversely affected many sectors in Turkey as well as all over the world. COVID-19, which affects the social and cultural areas as well as the finance area, has brought some risks in terms of banking. Banks, which are of great importance in the country's economy, have tried to take the necessary measures to protect themselves from the negative effects of COVID-19 and to perform their banking transactions in a healthy way. The banking system has struggled to achieve a stronger and resilient infrastructure during the pandemic period. In this study, the risky situations faced by the Turkish banking sector are examined; measures taken in banking activities, support packages and COSO components are introduced. With the pandemic, new/changing risks have entered our lives and the existing control mechanism may be missing. Therefore, measures should be taken against the risks encountered, regulations should be made, and control mechanisms should be reviewed.

With the pandemic, the use of technology has increased, especially in the field of banking.

In order to protect the health of customers and employees, digital channels were brought to the fore. These events have also shaped the risks encountered. With digitalization, fraud risks such as identity theft, cyber risks have increased. When we make use of the COSO Framework: It has been understood that the following should be done in the control of these risks; using

relevant information, communicating internally/externally, selecting and developing control activities- general activities over technology, deploying control activities through policies and procedures. Thus, it is given how to approach this risk, which has changed with the COSO Framework approach. It is important to implement these steps in order for the control processes to work more healthily. With the pandemic, not only digitalization has increased, but also working conditions have changed. It has been switched to a home/remote working environment. There have been significant changes in the control environment with remote work. Therefore, it is likely that previous controls will not work in the new layout. In this case, it is important to review the controls appropriate to the new environment. The remote working model has entered our lives more and has brought different risks. For example, the physical and psychological conditions of the employees, working conditions in the home environment, being away from technical support at home, concentration disorder. In our study, it has been examined which title of COSO, which presents the framework of the control mechanism with these changes, reveals a situation related to it. When we make use of the COSO framework: It has been understood that the following should be done in the control of these risks; selecting and developing control activities- general activities over technology, deploying control activities through policies and procedures, demonstrating commitment to integrity and ethical values, competence, enforcing accountability, establishing structure, authority and responsibility. Thus, it is given how to approach this risk, which has changed with the COSO framework approach. It is important to implement these steps in order for the control processes to work more healthily. Moreover, it is understood that control processes should be updated with developments. Then, it is given under which component these risks are evaluated in the COSO Framework used in the control processes and an approach is given to how they should be evaluated according to the principles of the framework.

Bibliography

[1] Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021). Covid-19 and cyber risk in the financial sector. www.bis.org.

[2] Al-Shetwi, M., Ramadili, S., Chowdury, T., & Sori, Z. (2011).Impact of internal audit function (IAF) onfinancialreporting quality (FRQ): Evidence from Saudi Arabia.African Journal of Business Management,5(27),11189–11198. https://doi.org/10.5897/ajbm11.1805.

[3] Arabacı, H., Yücel, D. (2020). COVID-19 Pandemisinin Türk Bankacılık Sektörü Üzerine Etkisi. Social Sciences Research Journal, 9 (3), 196-208.

[4] Bakkal, H., Kasımoğlu, A. İç Kontrol Sistemine Karşılaştırmalı Bir Bakış "Coso Ve Coco Modeli". Mevzuat Dergisi, sayı-178.

[5] BDDK(2020). Basın Açıklaması (Pandemi Dönemi Kararları hk).

[6] https://www.bddk.org.tr/Duyuru/Detay/728.

[7] Beybur, M., Çetinkaya, M. (2020). Covid 19 Pandemisinin Türkiye'de Dijital Bankacılık Ürün ve Hizmetlerinin Kullanımı Üzerindeki Etkisi. Uluslararası Batı Karadeniz Sosyal ve Beşeri Bilimler Dergisi, 4(2), 148-163. https://doi.org/10.46452/baksoder.829078.

[8] Curti, F., Gerlach, J., Kazinnik, S., Lee, M., Mihov, A., Barkin, T., Bishop, S., Carrivick, L., Cetina, J., Davis, N., Gluck, M., Gupton, G., Healey, J., Migueis, M., Morales, K., Mosser, P., Lazaryan, N., Parekh, H., Robinson, W., … Waszkelewicz, T. (2021). Cyber Risk Definition and Classification for Financial Risk Management. https://advisenltd.com.

[9] Dağıdır Çakan, C. (2021). COVID-19'un Türk bankacılık sektörüne etkisi. T. Münyas (Ed.), Verilerle pandemi sürecinde Türkiye (s. 215-240) içinde. Ankara: Nobel Yayınevi.

[10] Duran, M. S. ve Acar, M. (2020). Bir Virüsün Dünyaya Ettikleri: CoviD-19 Pandemisinin Makroekonomik Etkileri. International Journal of Social and Economic Sciences. 54-67. http://www.ijses.org/index.php/ijses/article/view/262/256.

[11] Gay, G., & Simnett, R. (2007).Auditing and assurance services in Australia. McGraw-Hill Irwin.

[12] Huremović, D. (2019). Mental Health of Quarantine and Isolation, in D. Huremović (Ed.), Psychiatry of Pandemics, A Mental Health Response to Infection Outbreak. Switzerland: Springer.

[13] ILO. (2020). COVID-19 Ortamında ve Sonrasında Uzaktan Çalışma Uygulama Kılavuzu.

[14] T.C Aile Çalışma ve Sosyal Hizmetler Bakanlığı, (2021). COVID-19 Döneminde Uzaktan Çalışma Yöntemi.

[15] Karluk, R. (2002), "Türkiye Ekonomisi: Tarihsel Gelişim, Yapısal ve Sosyal Değişim". Beta Yayınları, İstanbul.

[16] TBB, (2008). Bankalarımız 2008.

[17] Kocaman, B. (2021). COVID-19 Sürecinde Türk Bankacılık Sektörü Ve Piyasa Yoğunlaşmasının Analizi. Hitit Sosyal Bilimler Dergisi, 14(2), 384-407. doi: 10.17218/hititsbd.1007890.

[18] KPMG (2020a). Risk Management and Internal audit in times of COVID-19. https://home. kpmg/be/en/home/insights/2020/03/rc-how-riskmanagers-and-internal-auditors-can-help-in-times-ofcovid-19.html (05.01.2023).

[19] KPMG (2020b). 19 COVID-19 Risks: Insights Into A Changed Risk Landscape. Erişim Adresi: https://home. kpmg/be/en/home/insights/2020/04/rc-19-covid-19- risks-insights-into-a-changed-risk-landscape.html.

[20] Madendere, M.(2005). Kurumsal Risk Yönetiminde İç Denetimin Rolü, Çeviri/ Derleme.

[21] Melikyan, M. (2015). İşletmelerde İç Kontrol Sistemi Ve İç Kontrol Sisteminin Risk Azaltıcı Etkileri. T.C. Haliç Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Muhasebe Ve Denetim Bilim Dalı. Yüksek lisans Tezi.

[22] Olatunji O, Adekola D, & Isaac A. (2014). Analysis of Frauds in Banks: Nigeria's Experience. www.ijird.com.

[23] PWC, (2020). Implications of COVID-19 crisis for the Turkish banking sector.

[24] Payne, K., Foreman, D. (2021). 8 common bank scams (and how to avoid them). https://www.forbes.com/advisor/banking/common-bank-scams-and-how-to-avoid-them.

[25] Rezaee, Z. (1995). What the COSO Report Means for Internal Auditors, Managerial Auditing Journal, Vol. 10 No. 6, 5-9.

[26] Sebilcioğlu, F. (2020). COVID-19 sürecinde risk yönetimi ve iç kontroller. http://www.cerebra. com.tr/tr/covid19-covid19-surecinde-risk-yonetimive-ic-kontrolle.html.

[27] Sertkaya, B.,Baş, S. Covıd-19 Salgınının Türkiye Ekonomisi Üzerine Etkileri: Riskler Ve Olası Senaryolar. Dicle Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi Dicle University, Journal of Economics and Administrative Sciences ISSN: 1309 4602 / E-ISSN: 2587 – 0106. Yıl / Year: 2021 Cilt /Volume: 11 Sayı / Issue: 21 Sayfalar /Pages: 147-167.

[28] Sobel, P. J., Chambers, R. F., Murdock, D. C., Landes, C. E., Thomson, J. C., & Schandl, A. (2019). The Institute of Internal Auditors (IIA) Committee of Sponsoring Organizations of the Treadway Commission Preface COSO Board Members.

[29] Stuijfzand, S., Deforges, C., Sandoz, V., Sajin, C.T., Jaques, C., Elmers, J., Horsch, A. (2020) Psychological impact of an epidemic/pandemic on the mental health of healthcare professionals: a rapid review. BMC Public Health 2020; 20(1), 1230.

[30] T.C. İstanbul Valiliği, (2020). Cumhurbaşkanı Erdoğan "Ekonomik İstikrar Kalkanı" Tedbir Paketini Açıkladı. 18.03.2020.http://www.istanbul.gov.tr/cumhurbaskani-erdogan-ekonomik-istikrar-kalkani-tedbir-paketiniacikladi.

[31] T.C. Sağlık Bakanlığı. (2020). COVID19-GuvenlikGorevlilerineYonelikOneriler.

[32] The Institute of Internal Auditors. (n.d.). Iıa'nın Üçlü Hat Modeli: Üçlü Savunma Hattı İle İlgili Güncelleme.

[33] Toroslu,V.(2014). 6102 sayılı Türk Ticaret Kanunu Kapsamında İç Kontrol Ve İç Denetim. İstanbul: Vedat Kitapçılık.

[34] Türedi, H., Gürbüz, F., Alıcı, Ü. (2014). Coso Modeli: İç Kontrol Yapısı. https://dergipark.org.tr/tr/download/article-file/165866.

[35] TÜREDİ, H., & KOBAN, A. O. (2016). Coso İç Kontrol Modelinde Risk Değerlendirme Faaliyetleri. Öneri Dergisi, 12(46), 155. https://doi.org/10.14783/od.v12i46.1000010009.

[36] Uzunay V. (2007) "Avrupa Birliğinde ve Türkiye'de Kamu İç Mali Kontrol Sistemi ve Bu Alanda Yapılan Düzenlemeler", Ankara, BUMKO.

[37] Volz, D. (2016). Yahoo Says Hackers Stole Data From 500 Million Accounts İn 2014. Reuters. https://www.reuters.com/article/us-yahoo-cyber-idUSKCN11S16P.

[38] Yeşilçelebi, G. (n.d.). İç Denetim Bağlamında Covıd-19'un Kurumsal Risk Yönetimi Süreçleri Üzerine Etkileri (The Impact Of Covıd-19 On Enterprıse Rısk Management Processes In The Context Of Internal Audıt).

[39] Yetiz, F. (2016). Bankacılığın Doğuşu Ve Türk Bankacılık Sistemi. Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Nisan 2016; 9(2).

[40] Yetiz, F. (2021). Covıd-19 Pandemi Sürecinin Türk Bankacılık Sektörü Çalışanlarına Ve Müşterilerine Etkileri: Swot Analizi. European Journal Of Science And Technology. https://doi.org/10.31590/ejosat.83579.

[41] Williams C., Chaturvedi R., Chakravarthy K. (2020) Cybersecurity Risks in a Pandemic.

[42] URL: https://www.jmir.org/2020/9/e23692 DOI: 10.2196/23692.

[43] Willink, S.(2021). A new approach to compliance: What is compliance culture? Ideagen.

[44] https://www.ideagen.com/thought-leadership/blog/what-is-compliance-cultur.

[45] https://www.hurriyet.com.tr/ekonomi/bankacilikta-isler-degisiyor-41557399.

[46] (www.akbank.com.tr).

[47] https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

[48] https://www.theiia.org/