

## Research Article

# Implementation of Anti-fraud Strategy at Bank Sulsebar in South and West Sulawesi Province

Muhammad Fadli Mappisabbi\*, Hasniati, and Muhammad Akmal Ibrahim

Department of Public Administration, Faculty of Social and Political Sciences, Hasanuddin University, Indonesia

## Abstract.

Fraud is an act of deviation, often occurring in financial services institutions. Every financial services institution is expected to implement an anti-fraud strategy by considering the characteristics of comprehensive fraud potential and implementing a fraud control system. This study uses a qualitative method to analyze the implementation of anti-fraud strategies at Bank Sulsebar in South and West Sulawesi Provinces. Primary data sources are obtained from in-depth interviews with various informants who play important roles in implementing anti-fraud strategies. Secondary data relates to statistical data related to fraud. The data analysis technique used is interactive analysis. The results of the study found that the anti-fraud strategy at Bank Sulsebar was carried out by issuing a Director's Decree number: SK/068/DIR/K/XII/2024 concerning Standard Operating Procedures (SOP) for the Implementation of the Anti-Fraud Strategy of PT. Bank Sulsebar. Other prevention efforts are carried out by building anti-fraud awareness, carrying out verifications and surprise audits, and using fraud detection systems. In addition, the Know Your Customer and Know Your Employee policies have been implemented but have not been consistent. In detecting fraud, the whistleblowing system method is used, but its implementation has not been optimal. Investigations and reporting are carried out in accordance with applicable procedures. Sanctions are given by implementing zero tolerance for fraudulent acts. Evaluations are carried out periodically and continuously and various findings are followed up according to applicable mechanisms.

**Keywords:** implementation, strategy, anti-fraud

## 1. Introduction

Regulations and policies regarding fraud prevention have been established by the Indonesian Government. Reforms in the field of state finance have been implemented through a package of laws consisting of Law Number 17 of 2003 concerning State Finance, Law Number 1 of 2004 concerning State Treasury and Law Number 15 of 2004 concerning Audit of Management and Accountability of State Finance. All three are the foundation and guidelines so that state finances can be managed in an orderly, economical, efficient, effective, transparent and responsible manner by paying attention to a sense of justice and propriety. In line with this objective, Law Number 28 of 2009

Corresponding Author:

Muhammad Fadli Mappisabbi;  
email: mappisabbi@gmail.com

**Published:** 2 September 2025

**Publishing services provided by**  
**Knowledge E**

© Muhammad Fadli Mappisabbi et al. This article is distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use and redistribution provided that the original author and source are credited.

Selection and Peer-review under the responsibility of the 2nd Doctoral International Conference Committee.



mandates the realization of a state administration that is free and clean from corruption, collusion and nepotism. Continuing this Law, the Regulation of the Financial Services Authority of the Republic of Indonesia Number 39 / POJK.03 / 2019 is present as a guide for financial institutions in formulating anti-fraud strategies. There are four pillars to formulate an anti-fraud strategy set by OJK, namely 1) Prevention, 2) Detection, 3) Investigation, reporting, and sanctions, and 4) Monitoring, evaluation, and follow-up. But fraud prevention measures require a multi-dimensional strategy which means using other approaches to be able to analyze fraud prevention measures from various perspectives [1].

According to the world's largest anti-fraud organization, ACFE, fraud is defined as an act committed by one or more individuals, involving deception or causing error, and resulting in losses for individuals or other parties. There are three types of fraud schemes, namely corruption, asset looting, and financial statement fraud. Fraud can occur in financial conditions that are too good or too bad, where in this situation, fraud may be hidden due to self-confidence or decisions [2]. Fraud in the banking sector is one of the serious challenges that can threaten financial stability, institutional integrity, and public trust. Banking fraud refers to unauthorized actions that are carried out intentionally to obtain personal gain or harm other parties, either by internal parties (bank employees) or external parties (customers, third parties). In practice, fraud can occur in various forms, such as document forgery, abuse of authority, manipulation of financial reports, to engineering credit transactions.

Fraud cases in the banking world are one of the major problems that can damage the reputation and sustainability of a financial institution. Fraud can be interpreted as an intentional act to gain personal gain through illegal means, to the detriment of other parties. In the context of banking, fraud includes abuse of authority, fraud, embezzlement, and other illegal acts that can harm banks, customers, and the financial system as a whole. This phenomenon raises an urgent need for a strategy to prevent, detect, and handle such fraudulent acts, known as the Anti-Fraud Strategy [2].

The four pillars of anti-fraud strategy are sourced from the Financial Services Authority Regulation (POJK) Number 39/POJK.03/2019. This POJK regulates the implementation of anti-fraud strategies for commercial banks. The 4 pillars include a) Prevention; b) Detection; c) Investigation, reporting and sanctions; d) Monitoring, evaluation and follow-up. The explanation of each pillar is as follows. The first pillar, Prevention. This pillar focuses on efforts to prevent fraud through various policies and procedures that encourage ethical behavior in the organizational environment. This prevention can be

done through training to increase employee awareness, the establishment of a code of ethics, and internal policies that support honest and transparent behavior. The second pillar, Detection. Detection is a very important pillar in the anti-fraud strategy. By using the right technology and monitoring systems, banks can identify indications of fraud early. Detection involves the use of data analysis tools and regular internal audits to find potential irregularities that occur.

The third pillar, Investigation, Reporting, and Sanctions If there is an indication of fraud, then an investigation step must be taken immediately. At this stage, the information obtained will be analyzed in depth to identify the perpetrator and understand the modus operandi used. Transparent reporting and the application of sanctions according to the level of error are important keys in this process.

The fourth pillar, Monitoring, Evaluation, and Follow-up. The final stage is continuous monitoring and evaluation of the effectiveness of the anti-fraud system implemented. Banks must ensure that every policy and procedure is running well and follow up to correct any weaknesses. This evaluation is important to keep the anti-fraud strategy relevant and able to address the evolving fraud modus operandi. With these four pillars, the anti-fraud strategy aims to create a system that can prevent and reduce the potential for fraud in banking, as well as provide clear sanctions for the perpetrators.

Bank Sulselbar as one of the regional development banks that plays an important role in supporting the local economy in the South Sulawesi and West Sulawesi regions, is inseparable from the potential risk of fraud, both from internal and external sources. In facing this challenge, an anti-fraud strategy is an important instrument that must be implemented systematically and sustainably. This strategy includes prevention efforts, early detection, investigation, reporting, and evaluation of any indication of fraud that occurs. Financial Services Authority Regulation (POJK) Number 39 / POJK.03 / 2019 is a normative reference for banks in implementing a comprehensive anti-fraud strategy. However, the success of implementing this strategy is not only determined by the existence of regulations, but also by the quality of implementation in the field, organizational culture, human resource capacity, and adequate supervisory system support. Therefore, this study aims to analyze the implementation of the anti-fraud strategy at Bank Sulselbar in the Provinces of South Sulawesi and West Sulawesi.

## 2. Methods

This study uses a qualitative approach, with the aim of understanding in depth the process of implementing anti-fraud strategies at Bank Sulselbar in South and West Sulawesi Provinces. This approach was chosen because it is able to explain the phenomenon contextually and comprehensively based on the perspective of the subjects directly involved in the implementation of anti-fraud strategies. A qualitative approach allows researchers to explore in depth the meaning and perceptions of individuals towards a complex event or policy [3]. This study focuses on understanding anti-fraud practices based on the four pillars as stipulated in POJK Number 39/POJK.03/2019, including: prevention, detection, investigation and sanctions, as well as monitoring and follow-up. Primary data was obtained through in-depth interviews with key informants, namely structural officials, compliance division staff, and internal auditors of Bank Sulselbar. This research was conducted at the head office of Bank Sulselbar which covers the entire working area of South Sulawesi and West Sulawesi Provinces.

The data processing process was carried out through the stages of transcribing interview results, rechecking the validity of the data (triangulation of sources and methods), and compiling data into main themes based on the dimensions of the anti-fraud strategy. Data analysis was carried out using the interactive model approach from Miles, Huberman, and Saldana which includes four main stages, namely data collection, data reduction, data presentation, and drawing conclusions [4]. Data reduction was carried out by sorting relevant information, simplifying the complexity of the narrative, and categorizing findings based on indicators on each pillar of the anti-fraud strategy. Drawing conclusions was carried out after all data had been analyzed in depth to obtain a complete understanding of the implementation of the anti-fraud strategy in the Bank Sulselbar environment, as well as to identify obstacles and opportunities for improvement.

## 3. Results and Discussion

The implementation of the fraud queue strategy is based on the Financial Services Authority Regulation (POJK) Number 39/POJK.03/2019. This POJK regulates the implementation of anti-fraud strategies for commercial banks. The 4 pillars include a) Prevention; b) Detection; c) Investigation, reporting and sanctions; d) Monitoring, evaluation

and follow-up. Based on the research conducted, the following research results and information were obtained.

The research findings on the first pillar in the anti-fraud strategy focus on the prevention aspect which has been systematically implemented by Bank Sulselbar through various internal policies and programs. The main policy that is the reference for implementing this strategy is the Decree of the Board of Directors Number: SK/068/DIR/K/XII/2024 dated December 30, 2024 concerning Standard Operating Procedures (SOP) for the Implementation of the Anti-Fraud Strategy. In addition, there are also other internal policies, namely the Decree of the Board of Directors Number: SK/067/DIR/K/XII/2024 dated December 30, 2024 concerning the Company Guidelines (BPP) for Internal Audit and Anti-Fraud of PT. Bank Sulselbar. And Board of Directors Decree Number: SK/003/DIR/K/I/2022 dated January 15, 2022 concerning the Company Guidelines (BPP) Whistleblowing System of PT. Bank Sulselbar.

Through this policy, Bank Sulselbar has established an operational framework to prevent fraud in all work units, including branch offices in South Sulawesi and West Sulawesi. This effort is strengthened by the implementation of a zero tolerance policy, which emphasizes that all forms of fraud cannot be tolerated and will be subject to strict sanctions regardless of the magnitude of the losses incurred. All levels, from the Board of Commissioners, Directors, to employees, are required to sign the Integrity Pact and Code of Conduct routinely, both upon appointment and during the annual evaluation period.

In building anti-fraud awareness, Bank Sulselbar has implemented various employee awareness programs that include training, seminars, religious activities, internal media publications, and digital socialization through websites and internal bulletins. Socialization of policies and understanding of types of fraud is also carried out periodically to all employees. The implementation of the Know Your Employee (KYE) and Know Your Customer (KYC) principles has also become part of the prevention strategy, although based on internal audits, inconsistencies were still found in their implementation in several work units. In addition, anti-fraud training has been provided to all levels of employees, but specific training related to detection and investigation is still limited to internal auditors or examiners. This effort reflects the proactive approach recommended by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which states that prevention is more efficient than fraud detection or correction [5]. Practices such as anti-fraud training, strengthening the code of ethics, and internal transparency support integrity-based internal control, as stated in the principles of

organizational governance by the OECD [6]. This is also in line with the probability-based risk management approach, which places prevention as the first pillar of a comprehensive anti-fraud strategy [7]. The main challenges in implementing this pillar include the placement of employees who do not match their competencies, the length of work in one unit without rotation, resistance to change, and the difficulty in mapping the ever-growing risk of fraud. Other problems that contribute to obstacles are the low awareness of anti-fraud culture at the operational level, and the less than optimal monitoring system for employee personal risk factors. However, Bank Sulselbar has conducted individual employee risk mapping based on behavioral parameters, work positions, and socio-economic conditions to strengthen a proactive and sustainable fraud prevention strategy.

In the second pillar, namely detection, it shows that from the data that has been captured in the Fraud Detection System application, there are 208 transactions that have been caught which are considered suspicious transactions that are suspected of having indications of fraud from 3,128,750 transactions captured in the Fraud Detection System application since 2022-2025. In implementing this pillar, Bank Sulselbar has built a system and mechanism that aims to identify early indications of fraud throughout its operational network, including in areas far from the head office. One of the main methods used is the Whistleblowing System which is designed to be easily accessible to all employees. This system is equipped with a whistleblower protection policy, a clear reporting mechanism, and follow-up procedures.

TABLE 1: Report of Fraud Indications from the Whistleblowing System.

Year	Number of Reports
2021	15
2022	13
2023	15
2024	10
2025	4

Source: Bank Sulselbar, 2025

Based on the data from the fraud indication report from the whistleblowing system, there is a downward trend in the number of fraud indication reports. This indicates that the whistleblowing system is functioning well with the various reports available, in addition, if seen, the number of fraud indication reports in 2023-2024 has experienced a downward trend. Furthermore, regarding the whistleblowing system, a Verification

Team was also formed to conduct an initial investigation into each fraud report received through the system. To increase the effectiveness of detection, Bank Sulsebar also carries out surprise audits periodically in work units with high risk levels, which are determined based on risk mapping by the Risk Management Division. Not only that, the surveillance system is carried out secretly to test compliance with anti-fraud policies, both by internal units and involving external parties such as OJK, BPK, or KAP.

Information technology plays a crucial role in detecting potential fraud. Bank Sulsebar uses a Fraud Detection System (FDS) that is able to detect suspicious transactions based on deviations from customer transaction patterns. This system provides early signals of unusual activity and strengthens data-based monitoring capabilities. Bank Sulsebar implements a detection system through routine audits, utilization of a whistleblowing system, and IT system monitoring. Early detection of potential fraud is supported by the principles of internal monitoring technology and real-time data processing [8]. The whistleblowing system is an important tool in reporting incidents, as explained in the fraud triangle theory by Cressey, that pressure, opportunity, and rationalization are the main causes of fraud [9]. The use of data and technology also supports the concept of Data, Information, Knowledge, and Wisdom (DIKW), where data from audits and reporting is processed into information to detect fraud patterns [10]. In addition, the Core Banking System is also used to monitor customer financial positions and detect anomalies, especially in the credit sector. Although this system has made significant progress, a number of challenges remain. Among them are limited reporting due to concerns about retaliation, limited capacity of verification personnel, and less than optimal audit frequency across all branches. In addition, the evolution of increasingly sophisticated fraud modes, including those involving digital and cyber technology, requires continuous improvement of employee systems and skills. Therefore, adaptation and strengthening of technology-based detection systems and increasing digital investigative literacy are important steps in strengthening the Detection Pillar at Bank Sulsebar.

The research findings on the third pillar, namely investigation, reporting and sanctions, show that in the 2024-2025 period, there were 13 investigative audits that had been carried out in various branches and divisions, indicating a fairly broad scope in responding to indications of fraud. This reflects that the bank's internal early detection and reporting system is working effectively in identifying suspicious cases. In terms of reporting, all investigation results have been submitted to the Financial Services Authority (OJK) in accordance with regulatory obligations, but only one case was reported to

law enforcement, namely the Sengkang and Pare-Pare Branch cases in 2025. Regarding the perpetrators, the majority of fraud perpetrators were internal (11 out of 13 cases), while external perpetrators were only found in two cases, namely the Barru Branch and Sinjai Branch. Of the 13 cases investigated, 11 cases have been followed up, indicating efficiency in resolving fraud cases and implementing sanctions that are relatively timely.

Bank Sulselbar has built a systematic investigation system in handling fraud reports, including those originating from work units in rural areas. The process begins with an initial report by employees through the Whistleblowing System, which is then verified by the Verification Team under the coordination of the Internal Audit & Anti-Fraud Division. This team is tasked with testing the completeness and validity of the initial information before the recommendation is forwarded to the President Director to determine the need for further investigative audits. If the report meets the elements of alleged fraud, a comprehensive investigative audit is carried out, the results of which are reported to internal management (Board of Directors, Board of Commissioners, Ethics Committee) and also externally, especially the OJK. If a loss is identified to a customer or other party, the Bank is required to first replace the loss in accordance with the principle of prudence in order to maintain its reputation, while waiting for the final results of the investigation. This process also includes further monitoring of cases, loss recovery status, and sanctions imposed, which are coordinated periodically by the Internal Audit & Anti-Fraud Division.

The decrease in the number of branches audited each year, from 11 branches in 2021 to only 3 branches in 2025, is not due to a decrease in audit capacity. Instead, this decrease occurs due to the implementation of risk-based audits that focus on audits of branches with high risk profiles based on data analysis and previous case track records. This shows efficiency in the use of resources and the use of technology in detecting potential fraud before it occurs. However, although this approach can save resources, there is a risk that by relying entirely on a digital system, we can miss some indications of fraud that may only be detected through physical audits. Therefore, it is important to maintain a balance by conducting regular physical audits at branches that are considered to have a lower risk, to ensure that no errors or discrepancies are missed by the automated system.

In terms of external reporting, Bank Sulselbar consistently demonstrates compliance with reporting obligations to the Financial Services Authority (OJK), including reports of significant fraud incidents, semi-annual reports of anti-fraud strategies, and changes in strategy. However, for reporting to law enforcement, although there are channels and



coordination through the Corporate Secretary Division and the Anti-Fraud Division, the implementation is still discretionary. This means that the decision to bring a case to court depends on an internal assessment, taking into account the impact on reputation and the effectiveness of the legal process. Even so, the imposition of sanctions on perpetrators of fraud has been enforced with the principle of zero tolerance and imposed fairly, proportionally, and transparently by the Code of Ethics and Discipline Committee. Sanctions range from demotion to termination of employment, and compensation does not cancel the obligation to sanction.

In terms of sanctions against fraud perpetrators, there were two structural officials who were dishonorably dismissed after being proven to have committed fraud. One prominent case was from the Pare-Pare Branch, where the branch manager was proven to have abused his authority in credit management. Although this sanction was taken firmly, the organization's response to this dismissal was more secretive. There is not enough public information about the impact on the morale of other employees, which can affect their perception of the seriousness of the anti-fraud policy being implemented. As an improvement step, the organization needs to develop a more transparent internal communication mechanism, so that all employees know that the disciplinary policy is applied fairly and firmly. This is important to create a deterrent effect and strengthen the commitment to integrity at all levels of the organization.

This step reflects the principles of managing institutional integrity recommended by the United Nations Office on Drugs and Crime (UNODC) and the OECD [6,11]. The systematic investigation process, the establishment of the Code of Ethics Committee, and reporting to regulators reflect the integration between compliance and law enforcement. Although the procedures have been arranged, a number of challenges continue to hamper the effectiveness of this pillar. One of the main problems is the complexity of the investigation process, especially for technology-based fraud that is spread across various digital systems, while the capacity of digital forensic investigative human resources is still limited. In addition, inconsistency in reporting to law enforcement can reduce the deterrent effect. Internal coordination between units is also sometimes hampered, especially in tracking fraud that is cross-divisional or cross-regional. Another challenge is the length of the process of recovering losses from the perpetrators and the quality of legal evidence that needs to meet strict evidentiary standards in the justice system. Therefore, strengthening investigative capacity, accelerating legal processing, and improving the reporting system and internal coordination are priorities in continuously perfecting the implementation of this third pillar.

In the fourth pillar, namely monitoring, evaluation and follow-up, research findings show that in terms of audit recommendations, an average of more than 250 recommendations related to fraud are issued each year, with the actual number in the last period being 276 recommendations. Of that number, 242 recommendations have been followed up, 16 are in the process of being resolved, and 18 have not been followed up, so that the follow-up rate reaches around 88%, indicating a high level of response to audit results. The intensity of audits on branches shows a fluctuating trend: 10 branches (2023), 6 branches (2024), and decreasing to 3 branches (2025, as of May).

Bank Sulselbar has implemented a periodic and comprehensive monitoring system to assess the effectiveness of anti-fraud strategies in all work units, including branch offices in the South Sulawesi and West Sulawesi regions. This monitoring system is coordinated by the Internal Audit & Anti Fraud Division and is carried out with various frequencies, from daily to annually, depending on the level of risk and urgency of the fraud case that occurs. The form of monitoring implemented includes direct visits to work units, monitoring through internal systems such as the Core Banking System, and periodic reports from work units regarding the development of fraud cases. Information collected from monitoring results includes details of incidents, modes, actors, potential losses, and handling steps that have been or will be taken.

All monitoring results are discussed in the internal meeting of the Code of Ethics and Discipline Committee as a basis for evaluation and decision making. Fraud risk evaluation is carried out continuously through updating the risk profile mapping for each work unit, product, and operational activity. In addition, evaluation is also carried out in the preparation of the Annual Audit Work Program (PKAT) which uses the Risk Based Audit approach. Through this mechanism, the Bank can prioritize supervision of units or activities with a high level of fraud vulnerability. Annual evaluation through the Annual Audit Work Program (PKAT) and internal meeting discussions indicate the existence of a feedback loop in the internal control system [12]. The Code of Ethics and Discipline Committee meeting also functions as a forum to evaluate fraud incidents and formulate preventive measures in the future. Thus, the frequency of evaluation of potential fraud risks is not only carried out annually, but also occurs periodically and incidentally according to the dynamics of the case.

Follow-up on audit results that find indications of fraud is carried out systematically and comprehensively. The process begins with reporting the results of the investigative audit to the Board of Commissioners, Board of Directors, and Compliance Director within a maximum of three working days. Furthermore, this report is discussed in a Code of

Ethics and Discipline Committee meeting no later than seven working days after it is received. The results of the meeting include decision-making regarding the imposition of sanctions, demands for restitution of losses, and recommendations for improving the internal control system. If fraud is proven to have had a significant impact, the report must be sent to the OJK within the specified time limit. The follow-up process also includes further monitoring until the case is closed, including reporting progress to the regulator if necessary. Efforts to restitution losses are carried out in various ways, ranging from internal approaches to legal channels, such as asset auctions or civil lawsuits. However, the implementation of this fourth pillar is not without challenges. One of the main problems is the limitations of the real-time monitoring system in detecting digital fraud that continues to develop rapidly. Although monitoring is carried out with high frequency, the manual system and the separation of data between units still make it difficult to detect new fraud patterns early. In addition, integrating data from various sources (field visits, core banking systems, and unit reports) is a challenge in producing a comprehensive analysis. The follow-up of improvement recommendations has also not been fully implemented evenly across all work units, so the potential for similar modes to recur. Finally, measuring the effectiveness of anti-fraud strategies is still more focused on incidents that have occurred, while the measures to assess successful fraud prevention have not been fully developed quantitatively.

## 4. Conclusion

Based on the results of the study on the four pillars of the anti-fraud strategy at Bank Sulsebar, it can be concluded that this institution has implemented a fairly good system to handle fraud risks effectively. In the prevention pillar, Bank Sulsebar has succeeded in building an organizational culture that supports integrity, through the socialization of the code of ethics and strengthening internal control. Fraud detection is carried out through routine audits and the use of technology to monitor transactions, although there are still challenges related to the detection of new and sophisticated fraud patterns. On the investigation side, clear and comprehensive procedures are implemented, with monitoring of fraud follow-up through internal reports and external reporting to regulators such as the OJK. The monitoring and evaluation pillar shows that there are continuous efforts to identify and handle potential fraud risks, through risk mapping and discussions in internal meetings involving various related parties. However, the challenges faced by Bank Sulsebar are limitations in real-time monitoring

and data integration from various work units. Furthermore, although Bank Sulselbar has implemented an anti-fraud strategy in managing fraud risks, challenges related to technology, human resources, and the effectiveness of its implementation still need to be considered. For this reason, improving the monitoring system and strengthening capacity are very necessary to increase the effectiveness of the anti-fraud strategy as a whole.

The technical recommendations in this study are that digital fraud detection needs to be strengthened by integrating technology and machine learning to analyze more complex transaction patterns and detect anomalies in real-time. Second, the whistleblowing system should be expanded by using an independent third-party platform, to provide a sense of security and increase employee participation in reporting fraud. In addition, benchmarking with other regional banks that have more mature anti-fraud programs can provide insights for improvement. Furthermore, it is important to build performance indicators based on output and outcome, not just compliance with policies, to measure the extent to which anti-fraud policies are effective in preventing and detecting fraud. Finally, further research is needed to examine the factors that influence the effectiveness of the anti-fraud system and evaluate the technology and risk-based approaches applied in branch audits.

## References

- [1] Prabowo HY, Sriyana J, Syamsudin A. Anti-fraud strategy for Indonesian banking industry: an empirical investigation. *J Financ Crime*. 2018;25(3):870–85.
- [2] Association of Certified Fraud Examiners (ACFE). Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse. Austin (TX): ACFE; 2022.
- [3] Creswell JW. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 3rd ed. Thousand Oaks: Sage Publications; 2009.
- [4] Miles MB, Huberman AM, Salda na J. Qualitative Data Analysis: A Methods Sourcebook. 3rd ed. Thousand Oaks: Sage Publications; 2014.
- [5] COSO. Internal Control—Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission; 2013.
- [6] OECD. OECD Guidelines on Corporate Governance of State-Owned Enterprises. 2015 ed. Paris: OECD Publishing; 2015.
- [7] Arens AA, Elder RJ, Beasley MS. Auditing and Assurance Services: An Integrated Approach. 16th ed. Pearson; 2017.

- [8] Moeller RR. Brink's Modern Internal Auditing. 8th ed. Wiley; 2016.
- [9] Cressey DR. Other People's Money: A Study in the Social Psychology of Embezzlement. New York: Free Press; 1953.
- [10] Rowley J. The wisdom hierarchy: representations of the DIKW hierarchy. J Inf Sci. 2007;33(2):163–80.
- [11] UNODC. Anti-Corruption Ethics and Compliance Handbook for Business. Vienna: United Nations Office on Drugs and Crime; 2013.
- [12] IIA. International Standards for the Professional Practice of Internal Auditing. Institute of Internal Auditors; 2017.