Internal control system as a fraud management element in the company

Elena I. Efremova[1,*], *Elena I.* Zatsarinnaya[1], and *Anna A.* Soloshenko[2]

[1] Russian University of Economics named after G. V. Plekhanov, 36 Stremyanny Lane, Moscow Russian Federation
[2] JSC "Unicon", Varshavskoe Shosse, bld. 125 unit 1, section 11, 3rd fl., facility I, room 50, Moscow, Russian Federation

Abstract. The article examines the internal control system as an element of countering and combating corporate fraud in the organization, analyzes the possible risks of malicious actions in the organization strategic areas. The methods of internal fraud management in the organization are proposed. Internal control is a set of methods whose task is to evaluate the results of the organization's work, as well as control of the protection mechanism, which is aimed at preventing fraudulent actions, potential errors and violations. Internal control prevents falsification of accounting statements. Accounting and financial statements act as a link between organizations, investors, as well as other users of the organization's reporting. The reliability of accounting and financial statements is a decisive factor in making important decisions, because its falsification leads exclusively to losses for investors. Organizations often provide falsified reports, having a desire to show a more advantageous financial condition, to raise funds or conclude successful contracts. Falsification is always carried out with violation of legislation and regulations.

1 Introduction

Internal control is a set of analytical and control measures in the company, the results of which can significantly modify financial and managerial activities and affect the accounting methodology [1], which is why this complex can be associated with various ways to improve the organization efficiency [3]. For example, risk analysis and control that can lead to significant financial losses, ensuring the safety of assets, managing the organization obligations, as well as the prevention and detection of fraud and other illegal acts [2].

2 Materials and Methods

Such actions occur both in large corporations, where the organizational structure is complicated, and in small companies, but the owners and management of the organization are in any case interested in the proper use of all available monetary and non-monetary assets in the enterprise. That is, internal control mechanisms should meet the organizational

* Corresponding author: es-audit@mail.ru

structure of any complexity and identify fraud, inadequate or economically unjustified acts. Moreover, with the growth of the enterprise, measures to influence fraudulent schemes should also be improved. Due to the constancy of the control and methodological functions of internal management, such precedents can be minimized. There is also an independent study of EY company [4], which compares the degree of risk reduction in strategic areas where mechanisms have been qualitatively integrated into the organization's processes.

Fig.1. Reducing the risk of malicious actions in strategic areas where mechanisms have been implemented qualitatively.

Due to the demonstrated high efficiency of internal control mechanisms in identifying fraudulent risks, it is necessary to understand how its elements allow preventing illegal actions within the enterprise [5].

The first of them is the *control environment*. It provides rules and structure of events. Being the basis of the internal control system, it sets the pace for a huge number of processes in the company, including its corporate culture, control of management bodies, anti-fraud policy, mechanisms for punishing and encouraging employees involved in theft or detecting cases of unethical practices [6].

The next element is a *risk assessment*. The methodology of detecting fraudulent schemes, as well as further response to them, directly depends on this element.

Often, due to insufficient elaboration of this element, the internal control system at the enterprise does not function properly: there is no system for early detection and prevention of economic life facts that can reduce work efficiency [7]. This item requires a thorough approach to the development of evaluation methodologies, as well as a high level of competence of specialists due to the need for comprehensive knowledge of financial and managerial accounting, as well as the possibility of their application in practice.

Information systems ensure the circulation of potentially important data on the financial condition of the company, internal processes, information about the external environment, results of activities and communication processes with external users of reporting. A well-developed network of information and communication both within the organization and with the external environment ensures the proper speed of making managerial and financial decisions directly related to risky activities. As a rule, this is especially important in

complexly organized companies, where information must reach the top management bodies promptly to receive feedback or make a specific decision regarding urgent measures to reduce fraud risks.

Control activities include procedures related to the identification and protection of assets in the enterprise. In other words, it implements in practice the mechanisms developed in the risk assessment. This may include actions on documentary and ex post reviews, measurement, monitoring, separation of duties, information processing, protection from unauthorized access, and others.

At the moment, some companies are also resorting to the use of machine learning in controlling economic unjustified actions, as can be seen from *Figure 2*. IT solutions embedded in the management packages of internal control systems or proprietary risk analysis tools based on MS Excel are often used [8].

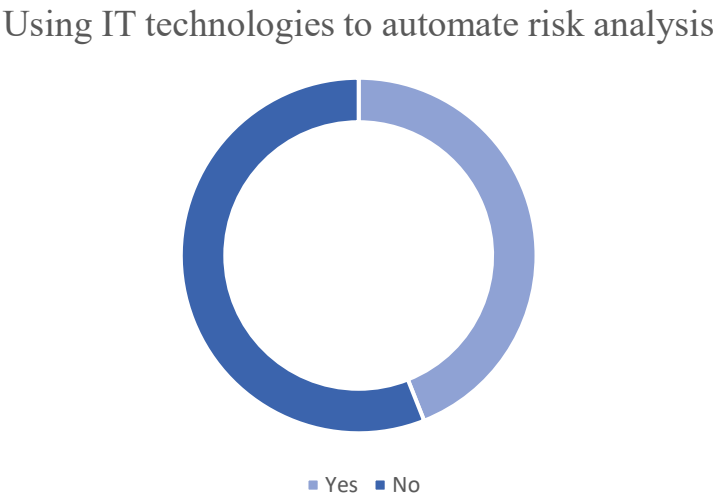

Fig. 2. The use of IT technologies to automate risk analysis in the company.

The mechanism is that the system detects anomalies in the presence of specific features in a single transaction that do not correspond to what is usually done in such situations. These models may become more widespread among companies in the future, since they are able to continuously monitor several facts of economic life at the same time.

However, simultaneously with the increase in the number of technological solutions used in the organization, the number of illegal frauds using information systems is constantly growing [3]. For example, in recent years, cases of phishing emails and interceptions of electronic mail systems have become more frequent, the means of protection against which may be the use of technologies to prevent leaks of confidential data, but the presence of such does not exclude the possibility of information theft, therefore, measures to inform employees about fraudulent schemes should be carried out on a regular basis.

The element of the internal control system is *monitoring*. Being continuous in carrying out, it is designed to monitor and give a reliable assessment of the entire internal control system effectiveness at the enterprise. This element includes all measures aimed at overseeing the daily activities of the company, the efficiency of all its systems, as well as the proper and competent performance of official duties by employees. Depending on the results of monitoring carried out on a regular basis and the risks identified during the work of the enterprise, the scale and frequency of inspections of the internal control service are built [8].

The head of the service notifies structural units of the planned inspections for them to prepare appropriate documentation that may be useful during control.

The five described elements of internal control represent a well-coordinated system of work between interrelated criteria for evaluating the work of the enterprise and personnel. At the same time, the internal control service is in continuous interaction with other departments, carrying out a continuous exchange of information. Thus, a whole set of tasks is performed: economic analysis, methodological support, consulting, development of management strategy and development of measures for anti-corruption impact in accordance with the risks of funds theft identified during the audit.

As a rule, the most common theft schemes are reduced to the fact that employees illegally appropriate the company's property. This applies to both cash and non-financial assets. Let's consider the most typical methods of fraud in these categories.

The theft of monetary assets can be carried out:

– directly by stealing cash from the cash register, subsequent concealment of the shortage, if the guilty person is responsible for the closure. During the internal audit, recalculation is carried out, as well as checking the cash register limit. There are also cases of falsification of accounting records to conceal the fact of theft, but due to the lack of payment documents, the scheme is detected during verification.

– making false requests for payment. A very common scheme of funds theft from personal accounts. Nevertheless, during internal control, external reporting documents are also requested, for example, settlements with suppliers and contractors. One of the variations is the development of false payment orders, fraud with bank transfers.

– using fictitious suppliers. A rather complex fraudulent scheme, but easily found by the characteristic features of such a transaction: the supplier company was created recently, the participants include interdependent persons, the one-time nature of the transaction and settlements through the same bank, intermediaries from both sides are involved. It will be difficult for the internal controller to assume the existence of such schemes at the first inspection, nevertheless, if the company is regularly monitored, then such precedents may be reflected in the internal audit log of a particular department or in the inspection reports for previous periods. This aspect reflects the importance of continuous monitoring and control, since fictitious transactions can be the basis for obtaining unjustified tax benefits and then the company will have to deal with the tax authorities.

– falsification of working hours to receive overtime payments. A complex scheme for detection, especially when it comes to types of work where labor costs are difficult to reliably determine with proper accuracy. Nevertheless, with the regularity and consistency of such payments, the controller is likely to have a question about the proper performance of duties by other employees and the reasons for overtime on a permanent basis.

– schemes aimed at manual adjustment of indicators in certificates, invoices, waybills, and other external documentation from suppliers and buyers. In this case, the decision of the internal controller to request documents from both sides for mutual verification is reasonable. In systems with electronic document management, unauthorized access to papers is practically impossible, which to a great extent simplifies the work of the internal control service [6].

3 Results and Discussion

In matters of this category, it is critically important to identify errors in a timely manner and correct them in accordance with the recommendations of internal controllers. In some situations, correction may be required urgently and less time is spent on audit report registration. In general, all detected violations are recorded and corrected in a given period of time. The responsible person, as a rule, is the head of the department, the correction period

is not unified and is imposed considering the specifics of the violation and the organization of processes at a particular enterprise. If a person involved in fraudulent actions is found, it is indicated in the report of audit findings with the name of the position held and the act committed. In some cases, the management is also provided with a memo. The Internal Control Service is not sanctioned, all further responsibility imposed on the employee will be initiated by the company's management and the law of the Russian Federation. Such procedures prevent not only the leakage of funds from the organization, but also the further accrual of fines by the tax control authorities.

Another category of fraudulent actions may be frauds with non-monetary assets of the company [6]. Such schemes are much more common in manufacturing or commodity companies, where, in addition to cash, assets are traded, sometimes falling into fraudulent schemes, including the following:

– falsification of inventory results or related other actions aimed at distorting the actually used stocks, goods, assets, as well as not reflecting them in sales accounting. In such cases, enterprises where the internal control service exists as a permanent unit significantly benefit. Members of the service can join the inventory commission, observe the actions during the inventory, make up their work records. In this case, the risk of discrepancy between the results obtained and the actual data is minimal, and therefore the fraudulent scheme can practically not be implemented. When checking sales accounting, the controller will need to check all payment documents on both sides to avoid overstating any indicators.

– the use of confidential internal corporate data for their own purposes. This may be the sale of any valuable information resources, usually from the category of intangible assets: databases, software, recipes, formulas, or the results of management analysis in that part of it that is a trade secret to third parties. As a rule, information technologies work best with these fraudulent schemes by blocking certain kinds of links, prohibiting access to certain information, the inability to send photos from corporate mail, notification of the presence of an unknown mailbox domain in correspondence [7]. This is one of the types of schemes, which is difficult to make public even if there is a constantly functioning internal control service; nevertheless, if such cases can be excluded in the future due to its recommendations to reduce the risk of information leakage, as well as a fraudulent scheme in this case.

– purchase of goods and services from the organization's counterparties at below-market prices for personal purposes using official position. The act may lead to an increase in economically unjustified expenses of the company and a further decrease in the effective distribution of funds. Such actions also include the inclusion of the employee's personal needs in organization expenses. For example, a full-time accounting employee with access to the company's personal accounts pays for his personal needs from them. To prevent this kind of fraud, the controller should check the expenditure transactions, as well as all documentation related to the purchase of goods and services in the name of the organization.

– unauthorized use of the company's private property. For example, the use of corporate transport for their own purposes and its subsequent maintenance is also at the expense of the company. In this case, the controller may also recommend a number of restrictions and rules, in addition to the existing internal regulations, which will facilitate the proper use of the property and control over damage that may be caused to it through unauthorized access.

– illegal changes in salary levels and related fraudulent actions are noticeable when checking settlements with staff. This can be both an overestimation of the payments level and an unlawful withholding of wages for a period of more than 15 days.

– exceeding the number of vacation days specified in the employment contract. When checking expenses, it is necessary to check the data on the accrual of vacation funds to employees and the period of their actual employment. This is not the most common type of fraud, since it is relatively easy to make public when checking internal documents.

– reimbursement of the same corporate expenses in several ways. As a rule, the doubling of accounting transactions is also easy to note when checking them. In addition, payment documents will confirm the presence of only one of them.

The identified facts of fraud and recommendations on countering them are sent directly to the management or owners, since these persons should be interested in the proper use of the organization's funds [9]. When detecting fraud on the part of management, the information must be transferred to the owners, except in cases where it is one person. In any case, the head of the internal control service is responsible only for providing audit reports within the established time frame, in accordance with his employment contract and job description. The responsibility assigned to him is disciplinary and he is accountable to the owners and managers of the organization.

It has already been mentioned that the availability of data for previous periods can significantly simplify the implementation of internal control measures due to existing precedents in the past. But, as the statistics in Figure 3 show, organizations often neglect the use of historical data for the correct operation of the internal control system.

As you can see, the vast majority of companies conduct results outside the system or in systems independent of each other, and therefore further countering fraudulent actions is significantly hampered by the lack of an accessible information base and the need for separate work on their processing and classification depending on the division [9].

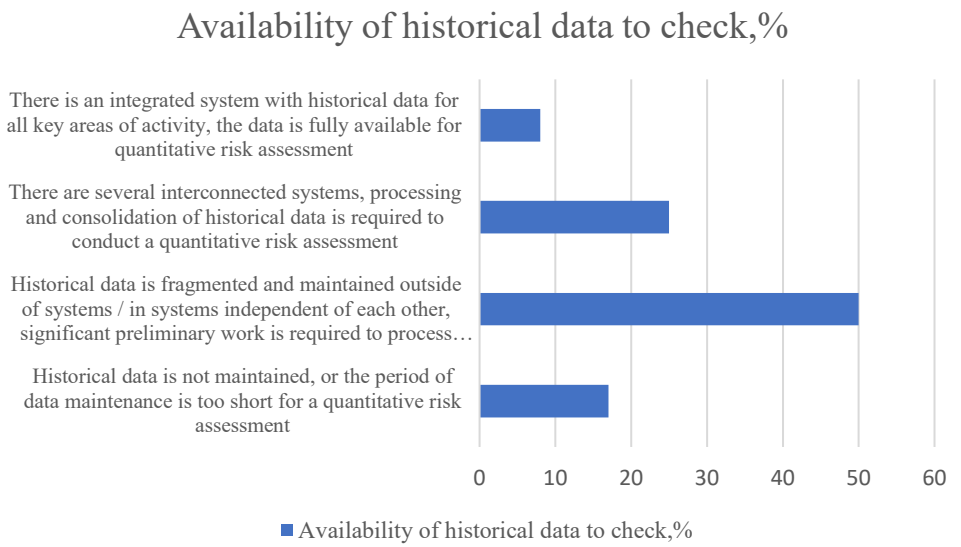

Fig. 3. Availability of historical data for verification by companies, % [3].

In the presence of integrated systems, the search area and the scope of information study are significantly reduced, it is much easier for internal control to distribute the work plan and the necessary measures to prevent fraud and theft at the enterprise. Nevertheless, there are a number of factors in the aggregate of which the internal control service is not able to provide effective protection of corporate assets from theft. According to the statistical data, the factors, depending on their distribution, are distributed according to *Figure 4.*

Fig. 4. Main areas of risk management improvement and internal control [4].

The majority of respondents noted that the integration of control systems in the strategic planning process could significantly increase the effectiveness of the activities carried out, and many also pointed to the need for more effective interaction between departments in the enterprise [10-12]. Integration work is already underway in these areas, as the companies note, so there is a possibility that in the future internal control in the context of activities to prevent fraudulent schemes will significantly improve the indicators for the number of identified facts of theft.

4 Conclusions

Thus, the internal control system at the enterprise, functioning as an integral system of interrelated elements, is able to effectively identify and prevent the facts of the organization's funds theft. Using monitoring and control mechanisms, there is a real opportunity to competently direct all monetary and non-monetary assets of the enterprise only for economically justified purposes. At the same time, the internal control service functions much more effectively as a permanent body. For example, it already has a certain database and a log of detected violations for the last inspection period, with the help of which it becomes possible to develop recommendations and methodological guidelines for structural divisions and internal control services for future inspection periods.

Nevertheless, the internal control service will not function effectively without a proper approach to its organization and provision of the necessary information resources. Often,

enterprises do not see the possibility of using internal control as a way to save the company's funds, but with the systematic and accurate work of all structures in cooperation, this system can help avoid a large number of problems, including with state structures, such as the tax service [5]. Separately, the introduction of automated internal control systems is often noted, but machine learning requires even greater requirements for historical audit data, so organizations need to competently organize an internal control system to prevent fraudulent actions right now.

References

1. E.I. Bakhtigozina, E. Efremova, E.A. Shevereva, A.A. Kurashova, E.I. Nalbatova, Fraud in the organization and direction of control in order to prevent it. Espacios, 39 (2018)
2. L.V. Dontsova, N.A. Prodanova, Risk-oriented approach in the practice of internal audit and control, In the book: Digital economy: trends and prospects of development. Collection of abstracts of reports of the national scientific and practical conference: in two volumes 226-229(2020)
3. Study of the current state and trends in the development of internal audit of financial organizations in Russia 2020 Joint research of IWA and PwC, IIA URL: https://www.iia-ru.ru/contact / (accessed: 08.12.2022)
4. Study of the current state and trends in the development of internal audit in Russia // IIA URL: https://www.iia-ru.ru/contact / (assessed: 10.12.2022)
5. E.I. Efremova, A.A. Kurashova, I.S. Medina, E.A. Fedchenko, M.L. Vasyunina, E.I. Bakhtigozina. Organization and functioning of the internal control service in an outsourcing organization. *Astra Salvensis,* 491-497(2019)
6. O.B. Ivanov, E.A. Egorova. The state and directions of development of internal audit, internal control, and risk management systems in companies with state participation//STAGE.2015.NO.6.URL: https://cyberleninka.ru/article/n/sostoyanie-i-napravleniya-razvitiya-sistem-vnutrennego-audita-vnutrennego-kontrolya-i-upravleniya-riskami-v-kompaniyah-s (accessed: 03/04/2023)
7. Research in the field of internal audit, risk management, internal control, and compliance in Russian companies with state participation, EY Assets URL: https://assets.ey.com / (accessed: 12.12.2022).
8. A.D. Khairullina, Yu.F. Volkova. Transformation of the organization's risk management system in the conditions of increasing uncertainty of the operating environment. Bulletin of Samara State University of Economics, **5(211),** 60-70 (2022)
9. E.M. Akhmetshin, V.L. Vasilev, D.S. Mironov, E.I. Zatsarinnaya, M.V. Romanova, A.V. Yumashev. Internal control system in enterprise management: Analysis and interaction matrices. European Research Studies Journal, **21(2),** 728-740 (2018)
10. N.A. Prodanova, N.S. Plaskova, E.I. Zatsarinnaya, S.H. Nabiev, N.V. Chumakova. Internal audit development priorities in Russia. Internal Audit Development Priorities in Russia. Paper presented at the Proceedings of the 35th International Business Information Management Association Conference, IBIMA 2020 - Education excellence and innovation management: a 2025 vision to sustain economic development during global challenges, (Seville, SPAIN, 2020) 6692-6696.
11. E.A. Osadchy, Development of the financial control system in the company in crisis. Mediterranean Journal of Social Sciences, **6(5S2)**, 390-398(2015). doi:10.5901/mjss.2015.v6n5s2p390

12. V.L. Vasilev, N.I. Vlasova, A.V. Kazakov, X.Y. Kotova, R.H. Ilyasov. Improving management functions at an enterprise: Levels of the internal control system. Quality - Access to Success, **20(171)**, 39-43(2019).