ЭКОНОМИКА: ИСТОРИЯ, ТЕОРИЯ, ПРАКТИКА
ЭКОНОМИКА: ТАРИХ, ТЕОРИЯ, ПРАКТИКА
ECONOMY: HISTORY, THEORY, PRACTICE

IRSTI 06.35.31
UDC 657.6:004
JEL H83

https://doi.org/10.46914/1562-2959-2023-1-1-11-23

B.O. TUREBEKOVA,*[1]
PhD, associate professor.
*e-mail: turebekova_bo@mail.ru
ORCID: 0000-0003-0946-9211
S.S. SAPARBAYEVA,[2]
PhD, associate professor.
e-mail: saulet71@mail.ru
ORCID: 0000-0003-1686-5052
S.K. BARYSHEVA,[3]
PhD, associate professor.
e-mail: bsk0trz@gmail.com
ORCID: 0000-0002-8229-9899
M.S. ORAZALINOVA,[3]
PhD, associate professor.
e-mail: maira_orazalinov@mail.ru
ORCID: 0000-0002-0193-2761
[1]Al Farabi Kazakh National University,
Almaty, Kazakhstan
[2]L. Gumilyov Eurasian National University,
Astana, Kazakhstan
[3]Turan University,
Almaty, Kazakhstan,

INTRODUCTION AND IMPROVEMENT OF IT AUDIT IN KAZAKHSTAN

Abstract

Audit acts as an element of ensuring the sustainability of the economic entity, reduces its information risks, given the complexity of the structure and functions of accounting. The article considers the foreign practice of IT audit (IT information technology) using special international standards such as COBIT and ITIL, gives a characteristic of the role, direction of IT audit development in Kazakhstan. IT-audit gives answers to questions of timing of updating of hardware and software, justification of its necessity, establishment of a unified system of management of IS monitoring. The questions of compliance of used information systems and technologies with the goals and objectives of the business, place and ratio of IS and business, ways to optimize investments, adaptation of Kazakhstan IT-audit system to international practice are considered. The study analyzes the optimal IT management, examines the main types and forms of IT audit as a preliminary phase of the study of the existing IS.

Key words: IT-audit, information technology, international standards, financial reporting, software.

Introduction

IT management is the main part of company's management. It guarantees the rational and effective improvement of all its interrelated processes. IT management provides a framework that connects IT processes, IT resources, and information with the strategy and goals of an economic entity. It allows maximize the use of information, increasing capitalization and gaining competitive advantages.

In the 60s of the last century, the introduction of information systems for accounting in the commercial sector led to the emergence of a new profession in the field of IT – IT auditor. Soon, the first professional Association of IT auditors were created «Electronic Data Processing Auditors Association». The goal of Association was to develop standards and best practices for conducting IT audits. Today, the audit of IT controls is a mandatory part of every independent financial audit.

Information technologies are developing too fast, so in two or three years they may not correspond to the current level of information systems. In this case, it is needed to upgrade, update the software, and replace the hardware. Currently, the relevance of this area of audit has increased dramatically. IT audit is required, for example, when connecting a new set of hardware or implementing new software. In addition, an IT audit can be conducted as an independent assessment of the quality of information systems, for example, when a contractor delivers work. IT protects entity from mistakes in accounting policies and helps conduct competent strategic planning for the development of this subject. Conducting an audit helps to prevent economic crimes within the organization, eliminates conflicts with tax and other state control services. IT is particularly important to conduct an audit when changing the company's management team, chief accountant, a head of IT services, implementing a new information system or software package.

The value of it audits is that, in addition to high-level independent expertise of solutions and development of optimization proposals, they can serve as an enterprise development planning tool. In search of answers, managers create their own internal audit services, invite audit companies, and seek advice from consultants.

The results of the IT audit allow evaluate the work of contractors and identify existing shortcomings. The data obtained during the audit process allows assess the risks of placing confidential information in the information system of an economic entity and understand how to minimize these risks. Thus, conducting an IT audit in an organization is a good way to understand and assess the business risks associated to information technology.

Materials and methods

The methodological basis of the study was a method of scientific knowledge as a method of theoretical generalization that found on the study of audit practice in Kazakhstan Republic and developed countries. There are some scientific approaches are used: literature analysis, comparative analysis, systematization and generalization. In addition, a qualitative exploratory research approach was adopted. This approach is appropriate way in studying expert practices like auditing in upgrade hardware and software, in justifying its need, in installing a unified management system to monitor the information system, as well as providing conclusions. At the stage of functioning of information systems, managers of an economic entity are interested in slightly different information: whether the information systems and technologies used correspond to the goals and objectives of the business; whether the business has become an appendage of the information system; how to optimize investment in IT.

Main provisions

These issues are particularly relevant in connection with the process of reforming accounting in accordance with (IFRS). The program provides for the formation of a system of accounting and reporting standards that provide useful information to users; linking the accounting reform in the Republic of Kazakhstan with the main trends in the implementation of standards at the international level providing methodological assistance to organizations in understanding and implementing the reformed accounting model.

Audit firms use various methods and techniques to reduce the cost of conducting an audit and improve its effectiveness. One of them is the use of information systems (IS) for audit activities.

The use of computer accounting data of the audited economic entity significantly improves the quality of the audit. Computerized audit procedures allow you to understand the accounting system of the audited entity, its organization, and to note the accounting segments that require special attention of the auditor. The use of information systems in audit makes IT easier to use analytical procedures, and information can be clearly presented in graphical form.

Despite the wide range of software offered for accounting, information about audit automation software is presented very sparingly. IT should be noted that all the listed audit software products are closed-type systems. These systems include software products that do not allow you to make any independent changes.

Literature review

The concept of «information technology» (IT) is defined by many scientists in different ways: according to A.N. Morozevich, B.A. Zhelezko, L.K. Golenda, «IT is a system of methods for collecting, registering, storing, accumulating, searching, processing and issuing documented information at the request of users» [1, p. 8]. I.A. Brusakova gives a similar definition, which reads: «IT is a technology for collecting, registering, transmitting, storing, searching, processing and protecting information» [2, p. 352]. According to V.V. Trofimova, «IT is a set of methods, production processes and algorithms of production and technical means United in a technological chain, the implementation of which provides the collection, storage, processing, output and dissemination of information in order to reduce the complexity of the processes of using an information resource, increase their reliability and efficiency» [3, p. 480]. N.S. Kosinenko says that «IT is a process that uses a set of tools and methods for collecting, processing and transmitting data (primary information) to obtain new quality information about the state of an object, process or phenomenon (information product)» [4, p. 304].

A.A. Sitnov asserts that IT should be understood as a system of rules that define the methods of collecting, accumulating, registering, transmitting, processing, storing, searching, modifying, analyzing, protecting, and issuing the necessary information to all interested departments or individual users [5, p. 240]. In article «Features of information infrastructure audit» he describes IT process audit as «audit of information technologies and systems that are critical for the implementation of a specific business process of an economic entity with specified quality and efficiency criteria». One of the most important results of this type of audit is a formalized model of the IT process under study and a specific business process.

Information technology management processes should be considered from the point of view of applying the methods of the best world experience. The most widely used approaches in this area are the following approaches to IT management: Cobit (Control objects for information and related technologies) and ITIL (IT infrastructure library). Both approaches are focused on meeting the needs of business units by the IT service and are based on a process approach, operating with measurable performance indicators. Cobit is a corporate information technology's tool that helps coordinate business and IT strategies as well as build a dialogue between business unit managers and information service management.

Due to the growing interest and need for IT audit, the approach to conducting IT has begun to take on orderly and standard form. With a support of major audit companies, associations of IT professionals have been organized to create and maintain standards for IT audit. In connection with a closure of these standards for General use and a growth of public interest in IT the Information Systems Audit and Control Association (ISACA) was established in 1967 to coordinate the actions of auditors and pool knowledge on IS management. The main goal of ISACA is to research, develop, publish and promote a standardized set of IT management documents for daily use by IT administrators and auditors [6, p. 240].

British standards institution defined the requirements for the service provider. The ISO 20000:2005 standard defines requirements for the service provider's service management system, ensures the quality of IT services for consumers. In 1986, the British government commissioned work on the

ITIL. This happened after the key role of the IT sector in the management of modern enterprises became apparent as computer technology developed.

The committee of sponsoring organizations of the Treadway commission (COSO) (USA) helps businesses and organizations evaluate and improve their internal control systems. The Committee of sponsoring organizations of the COSO is a standard that defines a system of requirements for improving the quality of financial reporting through effective management of the internal control system. These goals can be achieved by implementing recommendations and using best practices in the following areas: control environment, risk assessment, control procedures, information and communication, and monitoring.

The CMMI (Capability maturity model integration) standard is a collection of practical recommendations for improving software development processes. The Standard was published in America in 2002. In order to create this standard, an analysis of the key processes performed in software development and the risks associated with them was carried out [7]. CMMI allows an organization to evaluate the effectiveness of management processes, set priorities for their improvement, ensure consistently high quality of development, and implement these improvements.

The Sarbanes-Oxley act («SOX») was passed in 2002 as a result of a number of scandals with the reporting of large companies, primarily Enron. SOX became a forced measure- after Enron, WorldCom and some other reporting scandals, investors lost confidence in the correctness of the company's data.

In Western countries, information technology audits differ significantly from the CIS countries. «Federal information technology system» (FISCAM) offers a methodology for conducting control of information systems of state institutions in accordance with professional standards. FISCAM is intended for use primarily in certification activities conducted in accordance with GAGAS [8]. FISCAM is organized to facilitate effective verification of control over information systems.

Cyber incidents can cause significant damage to an organization. They can damage information assets and disrupt business operations. Some incidents lead to loss of performance others may lead to loss of consumer confidence, false reputation, and loss of trust or direct fraud [9]. However, information systems are part of critical infrastructure, so cybersecurity is part of the terrorist threat to national security. This makes it a top priority to manage information technology security and responsibility. Information asset protection includes not only protecting the intrinsic value of assets, but also preserving the confidentiality of confidential and established information and protecting the integrity of data and information stored in electronic form.

Huh B.G. and other revealed considering the use of information technology in corporations that quality of audit has improved through conducting informational system's audit in response to new types of audit risks that have emerged. The study confirms that an appropriate level of informational system audit input can improve audit quality [10].

Emerging technologies like data analytics and machine learning are anticipated in audit. Study presents an approach for applying audit data analytics and machine learning to full population testing and discusses related challenges [11].

Examination of the association between audit committee effectiveness, internal audit function and sustainability reporting practices by Huang F. and others indicated they are positively and significantly associated with sustainability reporting practices [12]. Tumwebaze Z. determined the concept of audit expectation gap as a multidimensional concept and identified different causes for the audit expectation gap as well as summarized several strategies into major promising strategies for narrowing it [13].

Otia J.E., Bracci E. provides evidence of an ongoing technological innovation within the audit. The changing environment triggered by technological advancements, increased demand for accountability and transparency means a change in the way auditing is done. The study analyzed and discussed how supreme audit institutions perceive and define the digital transformation phenomenon. The results show that most SAIs still do not master the concept of digital transformation, as they often refer to technology adoption or automation of auditing processes to be digital transformation, notwithstanding a great majority acknowledges the need for digital transformation but lacks the right strategy and resources in place. It proposed a general framework suitable for analyzing the factors involved in the DT in SAIs [14].

Results and discussion

Information technology management is the main part of the success of managing an economic entity, which guarantees the rational and effective improvement of all its interrelated processes. IT management provides a framework that connects IT processes, IT resources, and information with the strategy and goals of an economic entity, which allows you to maximize the use of information, increasing capitalization and gaining competitive advantages. Since then, the importance of the IT auditor profession has increased significantly. Today, the audit of IT controls is a mandatory part of every independent financial audit, IT audit services are in demand in the market, and large corporations have their own IT audit departments that periodically monitor IT processes and help improve them. At the same time, following the established standards and best practices is a prerequisite for conducting an audit in the most optimal way and with high quality.

Audit is a dynamically developing sphere in the economy of Kazakhstan. In accordance with the Law of KR (1998 No. 304-I) an audit is an independent audit of the accounting statements of an audited entity in order to express an opinion on the reliability of statements. Reliability refers to the degree of accuracy of financial statements, which allows the user of these statements to make correct conclusions about the results of economic activities, financial and property status of the audited persons and make informed decisions based on these conclusions.

IT features depending on the type of organization and its economic activity, directly affect the choice of the type and method of conducting an IT audit, the recommendations of the auditors, and the subsequent choice of IS and the corresponding II (information infrastructure). The features of the organization's functioning set the necessary minimum for creating an organizational management system. In turn, information system requires the use of appropriate IT and balanced II. Many factors influence the organization's management system, but the type of economic activity of the organization and its size play a significant role.

For example, when forming an information security policy, it is necessary to:

- identify the applicable legal documents, guidelines and standards in the field of information security, as well as the main provisions of the policy;
- identify approaches to risk management;
- structure counter measures by levels, etc.

However, the use of audit only in the study of countermeasures narrows its highly professional capabilities. It should be noted that only a comprehensive and systematic approach to the audit of an information system can have an appropriate effect. At the same time, an information security audit can only be an element of a business audit. The main targets of this audit are:

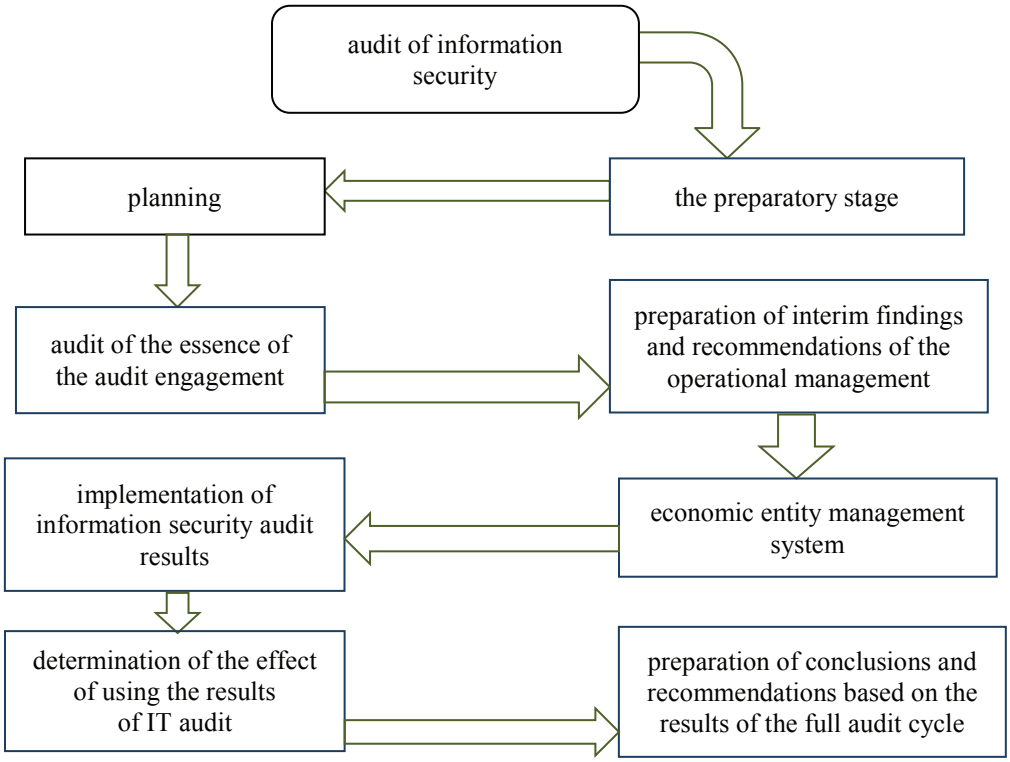
- research and analysis of risks related to the possibility of security threats against information technology resources;
- assessment of the current level of security of the information infrastructure of an economic entity;
- localization of bottlenecks in the security system;
- assessment of compliance of the information infrastructure with the existing requirements of information security standards;
- develop recommendations for implementing new and improving the effectiveness of existing information security mechanisms.

When organizing an information security audit, it should be taken into account that the audit cycle of research in this subject area involves the passage of five fundamental stages.

Information security's audit is realized stage by stage (Picture 1, p. 16), each of these stages has its own implementation algorithm.

The peculiarity of the organization of information security audit is a slightly different point of view on the collection and processing of information about the information infrastructure of an economic entity than in the audit of the state of information systems. For example, when defining the boundaries of an upcoming audit, the auditor should consider:

- list of physical, software, and information resources to be surveyed;
- premises that fall within the boundaries of the survey;
- organizational (legal, administrative, and procedural), physical, hardware, software, and other aspects of information security and their priorities on picture 1.



Picture 1 – Main stages of information security audit

Note: Picture drawn by authors.

When accepting an assignment to conduct an information security audit, the auditor should identify exactly the issues that are most important for this particular economic entity. For this purpose, it is important to carry out the preparatory stage, i.e. to define and agree with the management of this entity the specific goals and directions of the upcoming audit process. At the same time, the main role of the management of an economic entity as a person interested in the results of an information security audit is to provide comprehensive support to the auditor in clarifying the wording of the most significant problems for him, as well as in preparing sufficient and appropriate information support for the upcoming detailed audit study. Based on this, the specified stage should end with the most accurate formulation of the main problems facing the economic entity in relation to its information security and requiring mandatory solutions, as well as the conclusion of an agreement (contract) for conducting the specified audit in accordance with the task accepted by the auditor. Thus, the goal of this stage is to ensure unity in the understanding of the upcoming audit process by both the auditor and the client.

Main objectives of the enterprise information system audit: evaluate the effectiveness of the budget spent on IT tasks includes an analysis of the costs of specialists' salaries, capital expenditures (CAPEX) for equipment (per year), variable costs (OPEX) for licenses, subscriptions in services, hosting services, servers, and so on; evaluate the performance of the IT Department, as well as the overall level of training; identify places in the infrastructure and business processes where IT systems are not used effectively enough, develop recommendations for improving efficiency and reallocating the load; evaluate the performance of systems and processes that ensure the security of company data; assess the risks to the company's information assets and determine how to minimize these risks; ensure that all processes related to the IT system comply with industry laws and standards.

IT audit is a critical tool for determining problems at an enterprise in modern conditions of information society development, since the specified audit direction is a systematic process of obtaining and evaluating objective data about the current state of the IS and events occurring in IT, establishing the level of their compliance with a certain criterion and providing the results to the customer. IT allows correctly assess possible risks, predict failures, optimize the work of the IT Department, and solve many other tasks. Due to the lack of clear instructions in the Kazakh legislation in the field of

IT audit, most companies rely on common sense, international standards and «best practices» such as Cobit and ITIL.

Some types of IT audit are currently actively developing. Operational IT audit consists in reviewing the parameters of the functioning of the IT infrastructure at various levels: network; operating system; system software; software application; workflows; cryptography, etc. An IT resource placement audit involves reviewing buildings, server rooms where IT resources are located, including such aspects as physical security (walls, video surveillance, locks, security, entry procedures, etc.), environmental control (fire and leak protection, power supply, air conditioning), management systems, and IT equipment. During the audit of the developed IS, project management control, specification, development, testing, implementation of technical and procedural audits, classical information security checks of the developed system and corresponding business process checks are performed.

An IT management audit includes a review of organizational structure, strategy, work planning, resources, budgeting, cost control, etc. and, if applicable, an audit of relationships with external IT service providers. An IT process audit is an overview of the processes that occur within the IT Department, such as application development, testing, implementation, operations, maintenance, backup, support, incident handling, and so on. IT is obvious that most of the failures in the IT infrastructure due to inconsistent changes [15].

An information security audit involves performing checks related to confidentiality, integrity, and availability of systems and data. IT resource legality audit is a check of software licenses used, personal data protection, and compliance with regulatory requirements. Specific types of audit can also include an audit of the stability of the IT infrastructure to failures and disasters and special investigations, including author's checks performed to clarify the current situation of IT, related, e.g., to a takeover of new company and a need to merge IT infrastructure, debriefing, etc.

The existing international standards of management and audit in the field of information technology recommend evaluating any information system in terms of a set of IT processes, detailed control goals and standard operating procedures in order to determine whether the system meets the task of minimizing IT risks. This activity is considered both on issues specific to each individual IT process, and on standard elements of process management.

Requirements for the quality and reliability of the information contained in the financial statements are made by investors. That is confirmed by conducting a high-quality independent audit. It is carried out using clear and recognized procedures, which are based on the use of common approaches to the audit.

The difference between the International Standards on Auditing and those previously in force can be grouped according to a number of criteria. Differences of a formal nature are: the requirements of international auditing standards are disclosed directly in their text while clarifications to them are contained in separate annexes to the standards. Moreover, the structure and style of all international auditing standards is unified. The main fundamental advantage of international auditing standards is the use of a single approach to auditing, which is applied at the international level.

One of the advantages of standards over existing ones is their significant role in improving the quality of auditing and financial reporting. The need to adopt international auditing standards in our country was associated with the growing process of integrating domestic audit into the international community of auditors, as well as the increasing demand for audit services from foreign investors who already have investments or are just considering the possibility of investing in the economy of Kazakhstan.

In large audit organizations, it is built primarily depending on the organization's need for automation of its activities and material capabilities, because in comparison with small organizations to update the information technology of a large organization, the costs of research, writing technical specifications, development and implementation will differ in both time and money. It is recommended to choose a configuration that will be relevant for several more years and will be able to support the smooth operation of the IP. The difference for medium-sized and large organizations in the construction and configuration of it is and AI mainly lies in the scale and its structure. Types of IT audit systems that can be checked in table 1 (p. 18).

Table 1 – IT audit systems

Types of IT audit	What and how is investigated	Results
Express examination	During the survey, general data on the current state of IT infrastructure is collected and is structured.	Report with general description of the IT infrastructure as IT is at the moment, mostly on a superficial analysis and a set of minimum recommendations
Business process audit	The analysis of IT infrastructure is't carried out for the company as a whole, but only for a certain selected business process – an audit of computer hardware, of IT personnel involved in a business and audit of IT processes	Report on the current state of the process, recommendations on how to improve individual elements of the IT structure involved in this business process, how to bring them in line with standards and best practices for risk assessment.
Criteria audit	Collected and analyzed information on the IT system only in the context of a selected criterion, for example, IT audit on the performance, security, reliability, performance, etc.	Report with conformity assessment or inconsistency of the IT system to the selected criteria. In case of non-compliance, the reasons are analyzed and recommendations are given.
Multipurpose IT audit	The overall audit plan implies that the work of the IT infrastructure will be studied and evaluated comprehensively, as detailed as possible	Analytical reports on IT infrastructure, how much IT matches the details of the business as a whole and how strategic development should take place to match the business.
Note: Table compiled by the authors.		

The choice of the type and method of conducting its audit depends on the scale of the organization, the level of it development, and the desire of the organization's management to reach a higher level of competitiveness through it. The larger the organization, the more difficult it is to conduct its audit. This is due to the fact that the level of it in a large organization is usually higher than in a small business organization, where it is in its infancy and requires a rethink with a view to scaling, and it audit requires recommendations for optimizing and improving it. In this article, we will define what exactly we will understand by it audit.

The use of information technology in the course of an audit is one of the ways to improve the efficiency and reduce the complexity of the audit. A systematic approach to audit automation involves creating a unified information environment that all employees authorized by the project Manager can access. Thus, each user will have a certain level of access. Complex automation of audit activities involves the creation of an information system that will allow control all aspects of audit activities, not only conducting the audit itself, but also managing the audit firm as an economic entity with its economic and financial activities. Comprehensive automation allows monitor the quality of services provided at all levels, starting with audit, ending with the selection of employees and monitoring the costs of the entire company as a whole.

The concept of information security audit is currently not well established, but in this context IT audit can be represented as a process of investigation an information on IS of an economic entity in order to assess the level of its protection from permanent internal and external threats and develop management recommendations to minimize them. There are many cases when IT is advisable to conduct an information security audit, for example, when preparing a technical task for the design and development of an information security system, and after the implementation of the security system – to assess the level of its effectiveness.

The peculiarity of the organization of information security audit is a slightly different point of view on the collection and processing of information on an information infrastructure than on the audit of the state of information systems.

A special place in the government audit mechanism of Canada is awarded to «external» consultants. They are grouped together as acting consultants to the chief auditor. The group of experts on the protection of the environment immediately surrounds the environment and use it to his Council advises the auditor.

In Kazakhstan and Canada, you can identify the main differences by comparing the methods of conducting public audits. In accordance with the objectives and subjects in Kazakhstan, compliance

can be performed both independently and as part of the financial statements and performance audit.in Canadian practice, this type of audit is not traditionally performed and is an integral part of the audit of financial statements and performance audit. Of course, this approach to conducting compliance audits helps to reduce costs, and this in turn affects the progressive development of the economy and society as a whole, as it is aimed at modernization and optimization.

The rapid automation of outdated methods of work significantly increases the value of information technology for almost any type of business. Information has become a new type of financial asset that requires proper management. Timely and qualified response to the constantly changing landscape of IT and information security will prevent both direct losses associated with the compromise of information systems, and indirect losses that appear in the form of costs for eliminating security gaps, possible penalties from regulators or as a result of property penalties by court decision.

IT audit and information security services are provided throughout Central Asia: in the Kyrgyz Republic (Bishkek), Kazakhstan (Almaty), Uzbekistan (Tashkent), Tajikistan (Dushanbe) and Turkmenistan (Ashgabat). The result of our work is a description of the identified inconsistencies, a detailed methodology and evidence of their detection, as well as qualified recommendations for the elimination of identified risks. The main task is an unbiased definition and professional adjustment of specific information technology or security management processes, which allow the formation of vulnerabilities and inconsistencies.

According to the established practice, linear IT / information security managers and top management of the organization use the audit results to take concrete substantive measures to improve existing and implement current processes in the field of IT and information security management, for example:

- identify high-risk areas associated with the human factor and reorganize processes in such a way as to minimize or completely eliminate risks;
- make it possible to identify implicit risks, include them in existing risk management methodologies and outline an action plan to reduce risks to an acceptable level;
- allows to direct the vector of budget planning in IT and information security departments towards improving the efficiency of specific infrastructure components;
- total Cost of Ownership management allows define the boundaries of the effectiveness of IT solutions;
- effective use of systems is a direct consequence of compliance with the recommendations set out in the audit report.

Conclusion

Research has shown that information technology is becoming more complex every year. They consume huge financial and time resources. According to the research, it can be argued that each of the standards considered has a number of advantages: COBIT is more extensive and clearer, and ITIL describes the existing practices in more detail. In practice, both standards can be used together. They do not contradict each other, but complement each other. In practice, any of the selected approaches will require adaptation for the Kazakhstan market. Conducting an audit according to developed and adapted standards can be automated, because the audit process becomes a template. This will reduce costs and increase the efficiency of the audit. Both COBIT and ITIL do not take into account national characteristics, and additional adaptation of these standards is required for use in Kazakhstan. Automation tools should be developed for already developed and adapted approaches to conducting IT audits. It reduces costs and increases the efficiency of the audit.

Technical audit of information technologies is the collection, analysis of information and providing recommendations for improving the performance of a separate technical element of the information technology infrastructure. This type of audit is characterized by a small amount of work and a narrow technical specialization of the study.

When conducting an audit, a certain evaluation criterion was used to study not only a single element of the information technology infrastructure, but also the entire set of software, hardware, processes for their maintenance and maintenance in all the companies being audited.

Information technology security measures are necessary to minimize risks. In addition to protecting information assets, information technology security aims to maintain the confidentiality, integrity, and availability of information – important goals in government operations. Most government departments and agencies contain confidential information that requires access restrictions and confidentiality requirements that must comply with them. Data integrity is critical to ensure that program management and transmission is based on correct information. Information systems are part of the government's constructive infrastructure that provide online access to more services. Ensuring the availability of information systems is now important for the continuous service of the population.

The purpose of the audit was to assess the existing information technology security structure in the government to ensure uninterrupted maintenance and protection of information assets. Information asset protection includes not only protecting the intrinsic value of assets, but also preserving the confidentiality of confidential and established information and protecting the integrity of data and information stored in electronic form.

Now we live in a society that produces more information technologies than processed, stored, transmitted and any information. Extensive use of information leads to significant opportunities and benefits. At the same time, the widespread development of information technologies leads to serious threats to society about those who currently do not know. Information risks have great consequences both for society as a whole and for individuals. Thus, information security covers the entire society and is the concern of every person. According to the research, it can be argued that each of the standards considered has a number of advantages: COBIT is more extensive and clearer, and ITIL describes the existing practices in more detail. In practice, both standards can be used together. They do not contradict each other, but complement each other. In practice, any of the selected approaches will require adaptation for the Kazakhstan market. Conducting an audit according to developed and adapted standards can be automated, because the audit process becomes a template. This will reduce costs and increase the efficiency of the audit.

The issue of optimizing business processes in the Republic of Kazakhstan will be relevant as long as there are unprofitable enterprises in our country. An important point is the introduction of not just optimization processes in Kazakhstan's enterprises, but automated ones that meet modern trends and requirements. Buying a personal computer is not automation, a PC is just a tool.

IT audit allows to assess the compliance of information systems with business requirements and build a strategy for the development of information technologies. Often the reason for conducting an IT audit is the need to identify potential risks in the IT infrastructure. The issue of optimizing business processes in the Republic of Kazakhstan will be relevant as long as there are unprofitable enterprises in our country. An important point is an introduction of not just optimization processes in Kazakhstan's enterprises, but automated ones met modern trends and requirements.

REFERENCES

1 Морозович Л.К., Голенда Б.А., Зелечко А.Н. Компьютерные информационные технологии. – Минск: BGEU, 2003. – С. 56–63.

2 Брусокова Л.А., Шертовский И.Д. Информационные системы и технологии в экономике. – Москва: Финансы и статистика, 2007. – С. 152–153.

3 Трофимова В.В. Информационные системы и технологии в экономике и в управлении. – Москва: Юрайт, 2013. – С. 71–73.

4 Козиненко Н.С., Фризен И.Ж. Информационные системы и технологии в экономике. – Москва: Дашков и К°, 2012. – С. 204–206.

5 Ситнов А.А., Уринцов А.И. Аудит информационных систем. – Москва: ЮНИТИ-ДАНА, 2014. – С. 140–144.

6 Баранова О.В. Методологические подходы к аудиту информационных систем // Аудит и финансовый анализ. – 2013. – № 3. – С. 84–87.

7 ITGI. 2007. CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models, USA: IT Governance Institute. Global Information Security Survey. 2009. URL: http://www.ey.com/Publication/annual_GISS/$FILE/12th_annual_GIS S.

8 U.S. Government's 2017 and 2016 Consolidated Financial Statements // Financial Audit Manual. June 2018. Vol. 3.

9 Chow D.S., Humphrey C., Moll J. Whole of government accounting in the UK Project Report // Association of Chartered Certified Accountants. London, 2008.

10 Huh B.G., Lee S., Kim W. The impact of the input level of information system audit on the audit quality: Korean evidence // International Journal of Accounting Information Systems. 2021. No. 43. P. 1–24.

11 Huang F., Gyun N.W., Vasarhelyi M.A., Yan Z. Audit data analytics, machine learning, and full population testing // The Journal of Finance and Data Science. 2022. No. 8. P. 38–144. URL: http://creativecommons.org/licenses/by-nc-nd/4.0/

12 Tumwebaze Z., Bananuka J., Kaawaase T.K., Bonareri C.T., Mutesasira F. Audit committee effectiveness, internal audit function and sustainability reporting practices // Asian Journal of Accounting Research. 2022. No. 2. P. 163–181. DOI 10.1108/AJAR-03-2021-0036.

13 Deepal A.G., Jayamaha A. Audit expectation gap: a comprehensive literature review // Asian Journal of Accounting Research. 2022. Vol. 7. No. 3. P. 308–319. DOI 10.1108/AJAR-10-2021-0202.

14 Otia J.E., Bracci E. Digital transformation and the public sector auditing: The SAI's perspective // Financial Accountability &Management. 2022. Vol. 38. P. 252–280. URL: https://d-oi.org/10.1111/faam.12317 DOI: 10.1111/faam.12317.

15 Fiscal sustainability report. January 2017. URL: https://cdn.obr.uk/FSR_Jan17.pdf

REFERENCES

1 Morozovich L.K., Golenda B.A., Zelechko A.N. (2003) Komp'juternye informacionnye tehnologii. Minsk: BGEU. P. 56–63. (In Russian).

2 Brusokova L.A., Shertovskij I.D. (2007) Informacionnye sistemy i tehnologii v jekonomike. Moskva: Finansy i statistika. P. 152–153. (In Russian).

3 Trofimova V.V. (2013) Informacionnye sistemy i tehnologii v jekonomike i v upravlenii. Moskva: Jurajt. P. 71–73. (In Russian).

4 Kozinenko N.S., Frizen I.Zh. (2012) Informacionnye sistemy i tehnologii v jekonomike. Moskva: Dashkov i K°. P. 204–206. (In Russian).

5 Sitnov A.A., Urincov A.I. (2014) Audit informacionnyh sistem. Moskva: JuNITI-DANA. P. 140–144. (In Russian).

6 Baranova O.V. (2013) Metodologicheskie podhody k auditu informacionnyh sistem // Audit i finansovyj analiz. No. 3. P. 84–87. (In Russian).

7 ITGI. 2007. CobiT 4.1 – Framework, Control Objectives, Management Guidlines and Maturiy Models, USA: IT Governance Institute. Global Information Security Survey. 2009. URL: http://www.ey.com/Publication/annual_GISS/$FILE/12th_annual_GIS S. (In English).

8 U.S. Government's 2017 and 2016 Consolidated Financial Statements // Financial Audit Manual. June 2018. Vol. 3. (In English).

9 Chow D.S., Humphrey C., Moll J. (2008) Whole of government accounting in the UK Project Report // Association of Chartered Certified Accountants. London. (In English).

10 Huh B.G., Lee S., Kim W. (2021) The impact of the input level of information system audit on the audit quality: Korean evidence // International Journal of Accounting Information Systems. No. 43. P. 1–24. (In English).

11 Huang F., Gyun N.W., Vasarhelyi M.A., Yan Z. (2022) Audit data analytics, machine learning, and full population testing // The Journal of Finance and Data Science. No. 8. P. 38–144. URL: http://creativecommons.org/licenses/by-nc-nd/4.0/. (In English).

12 Tumwebaze Z., Bananuka J., Kaawaase T.K., Bonareri C.T., Mutesasira F. (2022) Audit committee effectiveness, internal audit function and sustainability reporting practices // Asian Journal of Accounting Research. No. 2. P. 163–181. DOI 10.1108/AJAR-03-2021-0036. (In English).

13 Deepal A.G., Jayamaha A. (2022) Audit expectation gap: a comprehensive literature review // Asian Journal of Accounting Research. Vol. 7. No. 3. P. 308–319. DOI 10.1108/AJAR-10-2021-0202. (In English).

14 Otia J.E., Bracci E. (2022) Digital transformation and the public sector auditing: The SAI's perspective // Financial Accountability &Management. Vol. 38. P. 252–280. URL: https://d-oi.org/10.1111/faam.12317 DOI: 10.1111/faam.12317. (In English).

15 Fiscal sustainability report. January 2017. URL: https://cdn.obr.uk/FSR_Jan17.pdf. (In English).

Б.О. ТУРЕБЕКОВА,*[1]
PhD, қауымдастырылған профессор.
*e-mail: turebekova_bo@mail.ru
ORCID: 0000-0003-0946-9211
С.С. САПАРБАЕВА,[2]
PhD, қауымдастырылған профессор.
e-mail: saulet71@mail.ru
ORCID: 0000-0003-1686-5052
С.К. БАРЫШЕВА,[3]
э.ғ.к., қауымдастырылған профессор.
e-mail: bsk0trz@gmail.com
ORCID: 0000-0002-8229-9899
М.С. ОРАЗАЛИНОВА,[3]
PhD, қауымдастырылған профессор.
e-mail: maira_orazalinov@mail.ru
ORCID: 0000-0002-0193-2761
[1]әл-Фараби атындағы Қазақ ұлттық университеті,
Алматы қ., Қазақстан
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Астана қ., Қазақстан
[3]«Тұран» университеті,
Алматы қ., Казақстан

ҚАЗАҚСТАНҒА IT АУДИТТІ ЕНГІЗУ ЖӘНЕ ЖЕТІЛДІРУ ЖОЛДАРЫ

Аңдатпа

Аудит экономикалық субъектінің тұрақтылығын қамтамасыз етудің элементі болып табылады, бухгалтерлік есеп құрылымы мен функцияларының күрделілігін ескере отырып, оның ақпараттық тәуекелдерін азайтады. Мақалада COBIT және ITIL сияқты арнайы халықаралық стандарттарды пайдалана отырып, IT-аудит (IT-ақпараттық технология) жүргізудің шетелдік тәжірибесі қарастырылады, Қазақстандағы IT-аудиттің рөлі мен даму бағытына сипаттама беріледі. IT-аудитті апараттық және бағдарламалық қамтамасыз етуді жаңарту мерзімдері, оның қажеттілігін негіздеу және АЖ мониторингінің бірыңғай басқару жүйесін құру туралы сұрақтарға жауап береді. Пайдаланылатын ақпараттық жүйелер мен технологиялардың бизнестің мақсаттары мен міндеттеріне сәйкестігі, АЖ мен бизнестің орны мен арақатынасы, инвестицияларды оңтайландыру жолдары, ҚР аудит жүйесін халықаралық тәжірибеге бейімдеу мәселелері қаралды. Зерттеу аясында IT-ны оңтайлы басқаруға талдау жасалды, қолданыстағы АЖ-ны зерттеудің алдын-ала кезеңі ретінде IT-аудиттің негізгі түрлері мен формалары қарастырылды.

Тірек сөздер: IT-аудит, ақпараттық технологиялар, халықаралық стандарттар, қаржылық есептілік, бағдарламалық қамтамасыз ету.

Б.О. ТУРЕБЕКОВА,*[1]
PhD, ассоциированный профессор.
*e-mail: turebekova_bo@mail.ru
ORCID ID: 0000-0003-0946-9211
С.С. САПАРБАЕВА,[2]
PhD, ассоциированный профессор.
e-mail: saulet71@mail.ru
ORCID ID: 0000-0003-1686-5052
С.К. БАРЫШЕВА,[3]
к.э.н., ассоциированный профессор.
e-mail: bsk0trz@gmail.com
ORCID ID: 0000-0002-8229-9899
М.С. ОРАЗАЛИНОВА,[3]
PhD, ассоциированный профессор.
e-mail: maira_orazalinov@mail.ru
ORCID ID: 0000-0002-0193-2761
[1]Казахский национальный университет им. аль-Фараби,
г. Алматы, Казахстан
[2]Евразийский национальный университет им. Л. Гумилева,
г. Астана, Казахстан
[3]Университет «Туран»,
г. Алматы, Казахстан

ВНЕДРЕНИЕ И СОВЕРШЕНСТВОВАНИЕ IT-АУДИТА В КАЗАХСТАНЕ

Аннотация

Аудит выступает элементом обеспечения устойчивости экономического субъекта, снижает его информационные риски, учитывая сложность структуры и функций бухгалтерского учета. В статье рассматривается зарубежная практика проведения IT-аудита (IT-информационная технология) с использованием специальных международных стандартов, таких как COBIT и ITIL, дается характеристика роли, направлению развития IT-аудита в Казахстане. IT-аудит дает ответы на вопросы сроков обновления аппаратного и программного обеспечения, обоснования его необходимости, установления единой системы управления мониторингом ИС. Рассмотрены вопросы соответствия используемых информационных систем и технологий целям и задачам бизнеса, места и соотношенияя ИС и бизнеса, путей оптимизации инвестиций, адаптации системы IT-аудита РК к международной практике. В рамках исследования дан анализ оптимального управления IT, рассмотрены основные виды и формы IT-аудита как предварительного этапа исследования существующей ИС.

Ключевые слова: IT-аудит, информационные технологии, международные стандарты, финансовая отчетность, программное обеспечение.