SILESIAN UNIVERSITY OF TECHNOLOGYPUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIESNO. 202

QUALITY MANAGEMENT SYSTEM AUDIT AND RISK MANAGEMENT

Katarzyna ZAWIERUCHA-KOZŁOWSKA

Faculty of Command Management, War Studies University, Warsaw; k.zawierucha@akademia.mil.pl,
ORCID: 0000-0002-9439-5589

Purpose: the article is an attempt to present topics related to management system auditing, as well as presenting the history of auditing in the world. The article also emphasizes the importance of conducting risk analysis in the context of a properly functioning quality management system.
Design/methodology/approach: the presented considerations indicated the growing position of management systems audit and certification, as well as risk analysis.
Findings: the article presents the history of the development of auditing and its industry universality as a way to verify the correct functioning of the organization. The conclusions also highlighted the growing importance of systems implemented into organizations.
Practical implications: the number of certificates issued indicate the great importance of international standards in the area of management systems of production and service organizations.
Originality/value: the information indicated shows the great importance of quality management, which provides many benefits for the organization. Additionally, the article presents the importance of audit in modern organizations, divides the audit and pays attention to the issue of risk and opportunity management, thus complementing the literature on the subject.
Keywords: audit, quality management, management systems, risk analysis.
Category of the paper: research and review publication.

1. Introduction

The increasing importance of quality in organizations has resulted in an obligation or recommendation to introduce a management system. Very often, the introduction of a system affects the competitiveness of the organization, strengthens its prestige and creates new opportunities. It also happens that the implementation of a quality management system becomes a necessity for the continued running of the organization. It may also be conditioned by regulations indicating meeting the restrictive requirements of the organization. However,

it is worth remembering that the correct functioning of the quality management system must be verified. Both by the organization's employees, including the internal auditor and a third-party auditor.

The basis for verifying the existing system is to conduct an audit. An audit is the most important and objective way of assessing a given process implemented in an organization (including quality control processes), a product, a project, a system or the entire organization. It can take three different forms:

— first page audit,
— audit of the other party,
— third party audit.

Guidelines for auditing management systems are included in the ISO 19011:2018 standard, which contains all the requirements for properly conducting an audit. This document contains the above-mentioned guidelines along with the principles of auditing, managing audit programs and conducting management system audits.

Additionally, as part of the audit, risk analysis is carried out in organizations, i.e. verification of whether the risk management process is carried out correctly. Risk management is one of the most important concepts of quality management. Together with the PDCA cycle (Deming cycle) and one of the principles of quality management - the process approach, it is the foundation for the proper functioning of the system and continuous quality improvement in the organization.

The ISO 9000:2015 standard also informs about opportunity management, so it refers to activities in the area of both risks and potential opportunities. However, attention should be paid to the flexibility of the standard in terms of its definition and the actions that should be implemented in the event of a risk or opportunity.

The aim of the article is therefore to present the issues related to the audit of the quality management system and risk and opportunity management, and to draw attention to the subjectivity of the interpretation of the requirements of international standards in this area.

2. Development of audit in the world

The issue of audit is undertaken by institutions, research centers and individual units. Audit plays a significant role in the functioning of enterprises, and its origins can be traced back several thousand years. The primary evidence for this theory are notes in stone from 3500 BC. created by writers living in the areas of ancient Mesopotamia. The obtained evidence indicates that during this period, control systems based on signs, e.g. punctuation (dots) or check marks, were already in use. They were placed next to the transaction amounts to verify payments. In addition to the areas of ancient Mesopotamia, similar systems were also used in Egypt, China

and Greece, where financial control was introduced, which could only be performed by an educated citizen with high social trust. Similar verifications were also carried out by two officials comparing their documents and records. This was to prevent money embezzlement (Winiarska, 2008).

In ancient times, the concept of audit was associated exclusively with the open presentation of the organization's accumulated assets through the so-called public reading of accounts. At that time, the auditor was a person who listened carefully to all the readings and, at the end, was obliged to express an opinion. These actions were intended to bring honesty to the people who were responsible for the organization's fiscal affairs. The auditors of that time were usually elected by the community, and the audit itself consisted solely of the already mentioned listening, because only a few at that time could read and write (Moeller, 2015).

In the times of the beginning of feudalism, no activities were carried out to confirm reliable keeping of financial books. Due to the developing trade in the 13th century in Italy, records of transactions began. Then the so-called double entry system, i.e. entering all transactions into the register and then transcribing them in chronological order, divided into columns: "owed" and "loans". It is also worth noting that auditing played a very important role at that time.

Then, during the decline of feudalism (16th-18th centuries), the scope of audit significantly expanded to include all transactions carried out by citizens managing processes in organizations and was carried out using the document verification method. At that time, efforts were made to detect and prevent all types of abuse by carrying out very detailed checks. In turn, the auditor had to be a competent person who could quickly detect errors, abuses and all types of fraud. Additionally, he had to have experience or skills in the area of accounting (Kołaczyk, 1996).

Initially, there were only internal audits, and their conduct in a manner similar to the modern one dates back to the period of the industrial revolution in England, when financial statements were controlled by checking the compliance of entries in the accounting books with the source documentation (Winiarska, 2008).

The enormous economic development at the end of the 18th and the beginning of the 19th century resulted in a significant development of enterprises and thus a reduction in the activities of factories. Mass production also meant an increase in the importance of financing sources and the importance of fixed assets, which also resulted in the increasing popularization of auditing and its gradual implementation around the world. At that time, the audit was carried out through dual activities. Firstly, as revealing frauds and errors, as practiced in Great Britain, and secondly, as a verification of the current financial condition and disclosure of irregularities. Ultimately, both forms were included in the scope of auditing (Montgomery, 1912).

The next important step in the development of auditing was the Great Depression of the 1930s, when on October 24, 1929, the Wall Street (American stock exchange) crashed, which resulted in the disclosure of the most spectacular bank frauds known to date in the world. As a result of these events, the United States Congress introduced new legal regulations. The Sucurities Act24 was passed in 1933 and the Securities Exchange Act25 in 1934.

This was of the greatest importance for the audit because on the basis of the above-mentioned legal acts, the Securities and Exchange Commission in the USA (SEC 26) was established. The commision's task was to ensure access to reliable information and reduce the risk associated with investing. At that time, financial statements were subject to approval by independent auditors, which led to the elimination of fraud and increased investor confidence in specific enterprises (Dasek, 2017).

The establishment of the Institute of Internal Auditors IIA in 1941 by 24 members was also significant for the evolution of auditing –founders of the Institute (Dasek, 2017). The primary role of the institution was to define auditing as a profession and treat it as a separate discipline shaping the image of the discussed issue.

Audyt wewnętrzny ma znacznie dłuższą tradycję niż dwa pozostałe rodzaje. Choć istnieje na świecie od bardzo dawna, w Polsce pojawił się dopiero w XXI wieku, kiedy wzmogła się intensywność przygotowań do wejścia Polski do Unii Europejskiej. Dlatego też można wyróżnić dwa etapy przygotowań do wprowadzenia audytu wewnętrznego do świadomości polskich organizacji. Pierwszy etap przypada na rok 2001 i dotyczy powołania instytucji audytu wewnętrznego na podstawie ustawy z dnia 27 lipca 2001 r. o zmianie ustawy o finansach publicznych, ustawy o trybie pracy Rady Ministrów, zakresie działania ministrów, Ustawa o działach administracji rządowej oraz ustawa o służbie cywilnej. Kontrola, o której mowa w ww. ustawie, została wprowadzona 1 stycznia 2002 roku ustawą o finansach publicznych. Powyższe przepisy obowiązywały do czasu nowelizacji ustawy o finansach publicznych w dniu 30 czerwca 2005 r. (CDB, 2014).

The ISO standard (International Organization for Standardization) 19011:2018 Guidelines for auditing management systems is also very important from the point of view of auditing management systems. It is intended for organizations that want to conduct effective and efficient internal and external audits of their management systems.

3. The importance of audit in the quality management process

The international standard ISO 19011:2018 defines audit as "a systematic, independent and documented process of obtaining audit evidence and its objective assessment to determine the degree to which audit criteria are met" (ISO 19011:2018). The guidelines contained in the standard, in addition to the guidelines for conducting the audit, also include information on the issue of assessing the competences of people carrying out the audit process. As the standard states, these activities include the person(s) managing the audit program, auditors and audit teams (ISO 19011:2018). As already mentioned, the following types of audits are distinguished (Table 1) (ISO 19011:2018):

— first party audit (internal audit) - carried out by the organization itself or on its behalf,
— second-party audit (supplier audit) – carried out by parties interested in the organization (by the organization's clients or other persons acting on their behalf),
— third party audit (certification audit) – carried out by independent auditing organizations (compliance registration/certification bodies or government agencies).

Table 1.
Basic differences between types of audit

Assumptions	First page audit	Second party audit	Third party audit
CONDUCTING AN AUDIT	mandatory audit	voluntary audit	mandatory audit/ voluntary audit
WYMAGANIA	compliance with ISO 19011 requirements	compliance with ISO 19011 requirements	compliance with the requirements of ISO 19011 and ISO 17021
IMPARTIALITY AND OBJECTIVITY	prohibition on auditing one's own work	it is advisable for the auditor to know the processes that are being audited	prohibition of cooperation with the auditee in forms other than audit
POST-AUDIT ACTIVITIES	auditor's participation in post-audit activities – dependent on the organization	auditor's participation in post-audit activities – dependent on the organization	prohibition of the auditor's participation in post-audit activities
AUDIT CRITERIA	audit criteria according to the ISO 9001 standard and organizational requirements	contractual audit criteria	audit criteria according to the ISO 9001 standard and organizational requirements
COMPETENCES OF AUDITORS	auditor competencies as defined by the organization	auditor competencies as defined by the organization	accredited auditor by the International Register of Certificated Auditors (the largest international certification body)

Source: own study based on data obtained during the Lead Auditor of the Quality Management System according to PN-ISO/IEC 9001:2015 course (CQI/IRCA PR328 Accreditation).

The scopes of audits vary depending on the type. A modern internal audit is an independent and objective assessment of the organization's activities, the aim of which is to increase the value and improve the operational processes of the enterprise. Internal audit, as already mentioned, is usually conducted by a designated employee of the organization with knowledge in the field of auditing or on behalf of the organization by a person from outside the organization. An internal audit should be conducted once a year to enable the organization to achieve its goals and protect it against improper management (Babuśka, 2005).

A second-party audit is carried out at the request of a potential or current subcontractor. This very often applies to cooperation with a supplier, when a production company decides to delegate processes to another company beforehand. Very often, such an audit is commissioned by companies with a quality management certificate among companies that do not have such a certificate, then the competences and the method of carrying out the entrusted activities are checked.

A third-party audit is carried out by certification bodies that confirm compliance of the management system with the requirements of the specified standards, e.g. ISO 9001:2015 confirming compliance of the quality management system. The entity carrying out this type of audit must be fully authorized to do so. The interested party, i.e. the organization applying for a certificate, selects a certification body (preferably one that enjoys an appropriate reputation and has conducted many third-party audits). There are the certification stages described below.

1. Selecting unit and sending a request for quotation.
2. Completing a certification application containing important questions about the organization, thanks to which the entity has a better opportunity to get to know the company in which the audit will be carried out.
3. Documentation review. The certification body reviews the most important system documentation, i.e. the Quality Manual, procedures, policies, instructions, etc., and then assesses the organization's qualifications to conduct an audit. Additionally, authorized persons answer questions sent by the unit that performs the initial qualification, thus preparing a report on the process.
4. Initial visit, which, based on the information received, may indicate irregularities in the functioning of the system.
5. Sending the audit program, i.e. its course plan, which is established by the certification body while agreeing on all requirements with the organization's representatives. Such a plan includes:
   — information about the auditee, i.e. the name and address of the auditee,
   — goal,
   — range,
   — criteria,
   — locations,
   — audit date,
   — duration with hours included,
   — audit team: lead auditor (name and surname), supporting auditor (name and surname), expert, specialist, observer,
   — people required/available during the audit on the auditee's side (positions, functions),
   — audit methods,
   — audit language and report language,
   — time and task schedule.
6. Conducting an audit, starting with the opening meeting, attended by people representing the certification body, headed by the lead auditor, and the top management of the organization. The aim of the opening meeting is:

— introduction of the audit team to the auditee,
— confirmation of the audit plan along with arrangements for logistic details,
— confirmation of the audit language and audit report,
— establishing the rules of communication during the audit and the method of transmitting information on audit progress and audit findings,
— reading the confidentiality, security, health and safety clause and others.
— providing information on the procedure for appeals, complaints, and conditions for interrupting the audit,
— determining the availability of resources,
— selection of the audit implementation method,
— sampling characteristics,
— characteristics of nonconformities, classification of nonconformities, consequences resulting from nonconformities,
— creating an attendance list of participants of the opening meeting.

The audit is carried out based on previously prepared criteria included in the audit program. The assessment of the functioning quality management system is made on the basis of the system's compliance with the international standard on which it is based, in this case the ISO 9001:2015 standard regarding the indicated system.

7. Completion of the audit - assessing the functioning of the quality management system of a given company at the closing meeting, and then creating a report on this basis. The audit report should include:
— number, date and place,
— identification of the auditee,
— purpose, scope, criteria, location,
— audit date,
— audit team with experts and observers,
— a list of people who took part in the audit on the auditee's side, along with observers,
— audit methods,
— audit findings and conclusions:
  - positive provisions, i.e. compliance,
  - areas for improvement/potential risks,
  - non-compliances (non-compliance card, description of non-compliance),
  - arrangements regarding the corrective action plan and other post-audit actions,
— signature of the lead auditor,
— signature (acceptance) of the auditee.

8. Obtaining a certificate - a positive assessment of the management system causes the lead auditor to apply for a certificate for the organization. The occurrence of non-compliance determines the improvement of the functioning of the indicated areas and the repeated application for granting a certificate, conditional on a positive assessment of the management system verified during the certification audit.

Audits are a valuable source of information about the correctness or irregularity of the functioning of a system or process, they indicate what needs to be changed and provide guidance on how to do it. An audit should not be equated with control, because its task is to improve the company's situation by identifying areas that do not function properly enough, and not only to verify errors. The audit should not be treated personally by the organization's employees. Functioning irregularities concern improper management, and thus provide an opportunity for development. A properly conducted audit has a positive impact on the process of continuous improvement, included in the indicated PDCA cycle (plan-do-check-act).

The number of certificates awarded is constantly increasing, and research shows that ISO 9001, ISO 14001, ISO 45001 and ISO/IEC 27001 are still the most popular ISO standard (Table 2).

Table 2.
Ranking of the number of ISO certificates issued

ISO standard	Number of valid ones ISO certificates in 2022	Increase in the number of ISO certificates compared to 2021
ISO 9001:2015	1 265 216	187 332 **(+17%)**
ISO 14001:2015	529 853	109 420 **(+26%)**
ISO 45001:2018	397 339	102 919 **(+35%)**
ISO IEC 27001:2013	71 549	12 862 **(+22%)**
ISO 22000:2018	45 459	9 335 **(+26%)**
ISO 13485:2016	29 741	2 512 **(+9%)**
ISO 50001:2018	28 164	6 257 **(+29%)**
ISO 20000-1:2018	27 009	15 240 **(+129%)**
ISO 37001:2016	5 969	3 073 **(+106%)**
ISO 22301:2019	3 200	641 **(+25%)**
ISO 39001:2012	1550	265 **(+21%)**
ISO 55001:2014	997	509 **(+104%)**
ISO 29001:2020	177	20 **(+13%)**

Source: own study based on: https://ikmj.com/ile-certyfikatow-iso-wydano/, 30.06.2024.

The presented research results indicate the current number of certificates awarded adapted to international ISO standards confirming the compliance of management systems. This is the number of certificates awarded by certification bodies accredited by members of the International Accreditation Forum (IAF). The conducted research also indicates that in the indicated period Poland took 18th place among 184 countries included in the ranking of the number of certificates issued (Figure 1).

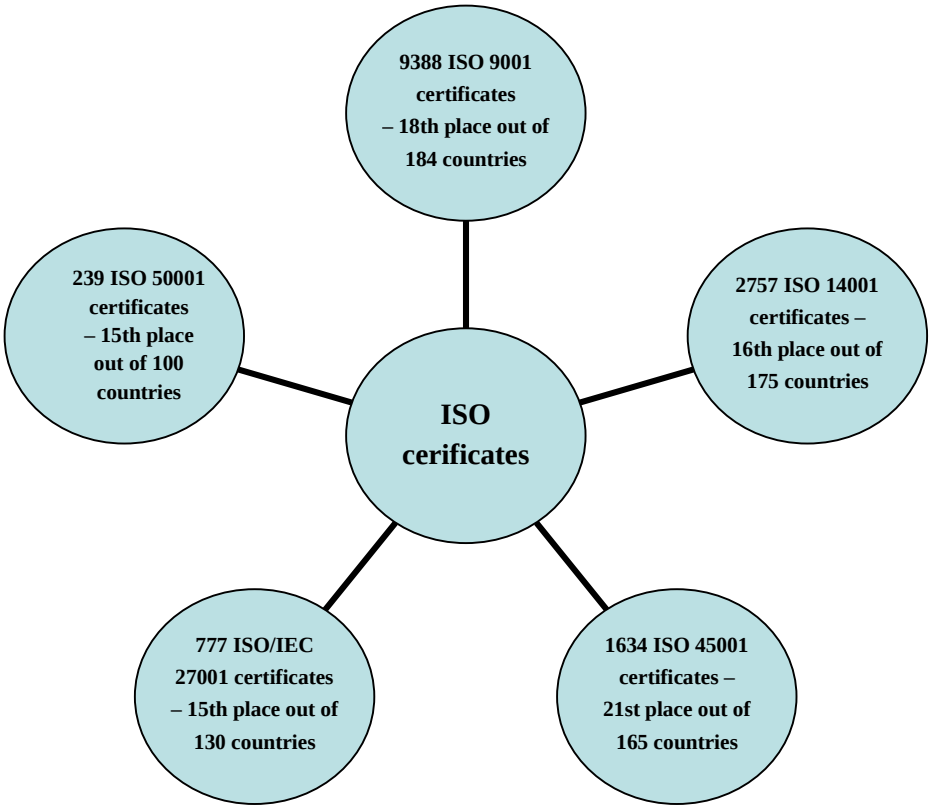

Figure 1. Number of ISO Certificates issued in Poland.

Source: own study based on: https://ikmj.com/ile-certyfikatow-iso-wydano/, 30.06.2024.

The number of ISO 9001:2015 certificates is 9388, which indicates the organization's greatest interest in the quality management system. It is also worth noting that the interest in certification in Poland is constantly growing, which proves the importance of quality for cooperating organizations and the huge importance of security of the environment, information, critical infrastructure, as well as employees and the local community.

4. Risk management as an improvement tool

Management systems based on international ISO standards, including the quality management system, are characterized by the same structure so that the basic points of the standards concern the same area. The unification of management system guidelines is possible thanks to the use of the so-called concept. "High Level Structure (HLS)", regarding the consistency of the main text, as well as concepts and definitions applicable to all management system standards. This concept is intended to facilitate the implementation of integrated management systems and the integration of the new system with those already implemented in the organization. Integrated management systems concern the functioning of many systems in

an enterprise, e.g. a quality management system, an environmental system and information security management, where all these systems form a coherent whole.

It is also worth noting that the HLS concept introduced into the system standards requirements regarding activities related to risks and opportunities, i.e. activities in the field of risk and opportunity management in the organization. This also applies to the ISO 9001:2015 quality management system standard. Taking into account the organization's production of high-quality products, risk is automatically limited, and the subjectivity of risk treatment means that the standard indicates a neutral approach to risk. This means that risk can be treated as a threat related to the loss of the organization's ability to achieve its goal or potential harm to the organization. However, the duality of risk may indicate the possibility of an opportunity for the company, i.e. it is likely that the organization loses something, but also gains much more than expected.

Risk itself is often defined in pejorative terms in the literature, but it is also pointed out that risk is the effect of uncertainty in achieving goals. This effect can be either a positive or a negative deviation from the expected goal. Risk is very often characterized in relation to a potential event and its consequences or a combination of event consequences (Wróblewski, 2011).

The ISO 9001:2015 standard introduces an approach to risk in terms of obtaining possible opportunities, specifying these requirements in point 6.1 Activities relating to risks and opportunities. Risk and opportunity management is therefore a basic element of planning the quality management system, the aim of which is to ensure compliance of the organization's functioning with current regulations and to minimize losses related to operational risk. Proper risk and opportunity management facilitates the planning of audit tasks and the identification of resource vulnerabilities, while also facilitating the process of estimating the effects of incorrect quality management. The most frequently encountered risks during the operation of an organization include (Wróblewski, 2011):

- economic slowdown,
- currency exchange rate fluctuations,
- changes in the legal/regulatory environment,
- fluctuations in raw material prices,
- interruption of activity,
- increasing competition,
- contractors - trade receivables,
- loss of reputation,
- cash flow/liquidity risk,
- data loss,
- disruptions/interruptions in the supply chain,
- civil liability/claims,
- failure to retain or attract talented employees.

When planning its quality management system influencing continuous improvement, an organization should first of all determine the sources of risks and opportunities included in the context of the organization and its obligations towards stakeholders. This verification therefore concerns internal and external factors important for achieving the set goals and their impact on the undertaken actions. In accordance with the requirements of the standard, attention should also be paid to the requirements of important interested parties identified during the examination of the internal, proximal and further environment of the organization. The requirements contained in the standard indicate that the analysis of the requirements contained in Chapter 4 of the standard, regarding the context of the organization, indicates that the identification of this point will allow for the accurate identification of risks and opportunities. However, it should not be forgotten that each risk and opportunity must be assessed by setting appropriate criteria relating to the consequences and probability of occurrence.

An important element of carrying out the described analysis is to inform employees about the possibility of a risk or opportunity for the organization. All employees should be aware of the actions taken and potential dangers or opportunities so that their actions are as effective as possible, which is conditional on planning actions related to risks and opportunities as well as ways of integrating and implementing these actions into the processes carried out in the area of the quality management system.

In accordance with the requirements of the standard, the organization should further assess the effectiveness of actions taken related to the described subject matter, along with reassessing the risk. Taking into account the results derived from the indicators developed by the organization and the simultaneous assessment of the management system by top management. In further analysis, the organization should implement corrective actions to address non-compliances that were revealed during the process of assessing the effectiveness of activities carried out as part of risk and opportunity management. In the event of non-compliance, the company should determine the cause of these non-compliances and implement corrective actions, i.e. verify the non-compliances and re-update the risks. The improvement process aims to reduce the level of risk and identify emerging opportunities.

5. Summary

Implementing a quality management system brings many benefits to the organization and strengthens its position against the competition, thus building its image among current and future customers. An audit of the quality management system requires presenting the organization's potential risks and opportunities to the lead auditor, so conducting regular analysis reduces the possibility of failure to achieve goals. Risk and opportunity management

is one of the most important elements ensuring the organization's process stability and further development in a constantly changing environment.

It is also worth noting that current trends indicate the potential of an integrated management system. Many companies choose more than one system regulated by international regulations in order to further improve and improve operational efficiency.

References

1. Babuśka, E. (2005). Audyt wewnętrzny w zarządzaniu przedsiębiorstwem. In: K. Winiarska (ed.), *Controlling i audyt w usprawnianiu zarządzania*. *Zeszyty Naukowe Uniwersytetu Szczecińskiego.* Szczecin.
2. Bednarek, P. (2009). *Historyczne uwarunkowania rozwoju audytu weenętrznego*. Wrocław: Uniwersytet Ekonomiczny we Wrocławiu.
3. Bednarek, P. (2014). Performance management In the Internal Audit Departments In Poland. *Olsztyn Economic Journal*. Olsztyn.
4. Bednarek, P. (2017). The relationship between organisational attributes and internal audit effectiveness. *Economic Journal Wrocław*. Wroclaw.
5. Bielińska-Dusza, E. (2011). Zakres pojęciowy audytu wewnętrznego. In: M. Lisiński (ed.), *Audyt wewnętrzny w doskonaleniu instytucji*. Warszawa: PWE.
6. CDB (2014). http://cdb.net.pl/historia-audytu/
7. Dasek, T. *Rewolucja audytu wewnętrznego na świecie*, https://www.repozytorium.uni.wroc.pl/Content/108610/PDF/04_Dasek_T_Ewolucja_audytu_wewnetrznego_na_swiecie.pdf
8. Kołaczyk, Z. (1996). *Rachunkowość finansowa*. Poznań: Wydawnictwo Akademii Ekonomicznej w Poznaniu.
9. Moeller, R. (2015). *Nowoczesny audyt wewnętrzny*. Warszawa: Wydawnictwo Nieoczywiste.
10. Montgomery, R.H. (1912). *Auditing Theory and Practice.* New York: Ronald Press Company.
11. PN-EN ISO 9001:2015 Systemy zarządzania jakością.
12. PN-ISO/IEC 19011:2018 Wytyczne dotyczące auditowania systemów zarządzania.
13. Winiarska, K. (2008). *Audyt wewnętrzny*. Warszawa.
14. Wróblewski, R. (2011). Risk management in the enterprise. *Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach.* Siedlce.