СТАТТІ

ARTICLES

_____

Sergiy Ivakhnenkov

https://orcid.org/0000-0001-7788-8659

DEVELOPMENT OF A CONCEPTUAL METHODOLOGY FOR PERIODIC AUDIT OF ACCOUNTING INFORMATION

Abstract

Purpose of the research. The purpose of this article is to develop methodologies for the continuous control and auditing of financial and accounting information amidst the rapid advancement of hardware and software technologies that enable real-time electronic reporting. The research aims to describe modern technologies applicable to continuous auditing and data analysis, specifically to ensure the reliability of information generated by information systems. It distinctively examines the concept of "periodic audit" as an alternative to embedded control modules, deeming it particularly relevant for the Ukrainian context.

Methods of the research. The article employs an analysis of current research and publications on real-time reporting and continuous auditing, referencing works by American and Canadian researchers and professional organizations (AICPA, CICA, Institute of Internal Auditors). It reviews theoretical frameworks for implementing continuous control and conceptual models of periodic audit. Electronic reporting standards, notably XBRL, and their implementation practices globally and in Ukraine are analyzed. Technologies for obtaining, verifying, loading, and analyzing data for periodic audit purposes are described, including statistical methods (trend analysis, regression analysis, cluster analysis, etc.). Data from surveys of Ukrainian enterprises regarding the online publication of financial statements are also utilized.

Results of the research. The study demonstrates that while technology facilitates real-time reporting, it necessitates corresponding continuous control and auditing to assure information reliability. Traditional continuous audit approaches involving embedded control modules in ERP systems present significant drawbacks: risks to system stability, high implementation costs, and limited developer support. The concept of "periodic audit" is proposed as an alternative. This approach involves periodically (e.g., nightly) extracting transactions into a separate data warehouse for subsequent analysis using specialized audit software. This enables near-continuous assurance regarding information, irrespective of the effectiveness of the enterprise's internal controls. A general model for acquiring data for periodic audit purposes is presented, encompassing data verification, correction, loading, and analysis stages. The primary goal of data analysis is identified as developing patterns to detect unexpected data or transactions indicative of fraud or errors.

Possible application of the research results. The proposed "periodic audit" methodology can be applied by internal and independent auditors to provide near-continuous assurance regarding the reliability of financial and accounting information generated by corporate computer systems. This approach is particularly beneficial in environments with inadequate internal controls, such as in Ukraine. The technology is versatile for identifying significant internal control weaknesses across various conditions, enterprises, information systems, and business/accounting structures. The results can inform the enhancement of audit practices, improve financial reporting quality, and enable the timely detection of fraud and errors.

Conclusions. Rapid technological development necessitates a shift towards continuous or near-continuous control of financial information. The "periodic audit" concept, involving regular analysis of data extracted to a separate warehouse, offers a practical and compromise alternative to embedded continuous control systems, especially where resources are limited or internal controls are weak. This approach allows auditors to provide timely assurance with minimal delay. Despite their advantages, continuous control and periodic audit systems have limitations, including the risk of failing to detect errors (false negatives) and generating false alarms

(false positives). Successful implementation requires an understanding of business processes and appropriate internal control technologies. The periodic audit concept holds particular relevance for Ukraine, given the need to improve management and control practices.

Keywords: Financial Reporting, XBRL, Financial Accounting Systems, Enterprise Resource Planning (ERP) Systems, Audit, Continuous Auditing, Periodic Auditing.

JEL classification: M420

Introduction and Problem Statement. Technological progress has significantly impacted the processing of financial transactions by computer systems; advancements in computer technology allow for faster retrieval of financial and operational information. Users can now obtain detailed and timely financial information about a company and assess its performance without waiting for quarterly or annual financial statements. Sometimes, users have direct access to databases containing the company's financial and operational information and can select the necessary data themselves. However, continuous reporting requires continuous auditing and control of such information.

Analysis of Recent Research and Publications. Real-time reporting of financial and non-financial information via corporate information systems and websites (and the need for auditing it) is rapidly increasing. In the USA, the Securities and Exchange Commission (SEC) is discussing the more active implementation of real-time corporate reporting systems. Under such systems, analysts and investors would have continuous direct access to information containing key financial indicators for timely financial analysis. In a study on this topic, American researchers led by Hunton (Hunton et al., 2002) reported that monthly, or even better, daily reporting would significantly enhance the usefulness of financial statements for decision-making, improve the quality of income reporting, and reduce management's aggressiveness regarding accounting accruals, estimates, and principles. As Vasarhelyi et al. note, the motivation for real-time reporting is that it could solve the problem of "managed earnings," as daily or weekly earnings would be harder for managers and financiers to manipulate than quarterly ones (Vasarhelyi et al., 2002). Furthermore, stock price volatility might decrease, analyst consensus on future earnings estimates could improve, and the cost of capital might decline.

Unresolved Parts of the Problem. The rapid improvement of hardware and software technologies has made real-time electronic reporting possible and affordable. However, continuous reporting (daily as well as monthly) requires continuous monitoring of such reports and assurance regarding the reliability

of the resulting information for users. Therefore, audits must also be continuous or performed at very short intervals.

Purpose and Objectives of the Article. The consensus on the definition and understanding of continuous auditing among foreign experts has not been matched by the development of corresponding methodologies. We believe this is because the discussion largely revolves around technologies for verifying transactions as they are executed in business processes, which pertains more to internal control than to independent (or even internal) auditing, although auditors can actively utilize these technologies. Our goal is to describe modern technologies that could be utilized in continuous auditing and data analysis.

Main Research Results. Currently, the most widespread standard for electronic reporting globally is XBRL (eXtensible Business Reporting Language). XBRL is supported by a dedicated consortium, XBRL.org, which includes major financial and auditing firms, as well as software development companies. The XBRL format is equally convenient for submitting mandatory reports to government regulatory bodies and for presenting reports on company websites. XBRL is an open specification based on the Extensible Markup Language (XML), utilizing generally accepted financial reporting standards and practices to prepare and exchange company reports in a unified format. An XBRL report is developed with two interconnected modules: a program for data retrieval and calculation execution, and a display form. Data exchange between the calculating and displaying parts of the report occurs in a special XML format, independent of the report user's computer system. The XBRL standard regulates the creation of "taxonomies" – dictionaries of reporting forms for various industries.

Reporting in XBRL format is becoming increasingly prevalent. For instance, the U.S. Securities and Exchange Commission (SEC) has accepted reports in XBRL format from securities issuers since 2005 (and made it mandatory from 2009), while statistical offices in Ireland, the Australian Taxation Office, and many other

institutions worldwide have also implemented the submission of quarterly statistical reports in XBRL. These issues are also relevant for Ukraine, which first introduced XBRL in 2021. Surveys of Ukrainian industrial, trading, and service enterprises, conducted by the Faculty of Economic Sciences at the National University of Kyiv-Mohyla Academy (NaUKMA) between 2014 and 2019, showed that more than a third of the surveyed business entities were already publishing their financial statements on the Internet (see Table).

On December 27, 2019, the Ministry of Finance of Ukraine approved the Ukrainian financial reporting taxonomy, Taxonomy UA XBRL IFRS 2019, which defines the composition of items and indicators of financial statements that reporting entities are legally required to prepare in accordance with international standards, using a single electronic format.

However, continuous reporting (daily and monthly) requires continuous control of the quality of such reporting. Some authors (Helms, 2002) argue that in paperless systems, continuous auditing is also necessary because transaction records (database transactions) and other files might disappear before the end of the reporting period. For example, Internet service providers hosting cloud systems on web servers may only store transaction data for a limited time. If data is not checked continuously, the auditor might simply miss it.

The concept that audits should also occur continuously or at very short intervals was developed by several American researchers. Professor Vasarhelyi and his colleagues at Rutgers University in New York have presented and advocated for the application of continuous auditing for many years. They also proposed a generalized concept of continuous auditing (though without specifying the operational model for practical implementation).

Let us clarify the concepts of continuous control and auditing. According to the Institute of Internal Auditors, continuous auditing is any method used by auditors to perform audits on an ongoing or continuous basis. S. Groomer defines continuous auditing as "a process or technique that allows independent auditors to provide assurance on substantive matters using a series of audit reports issued simultaneously with, or a short period of time after, the occurrence of the events underlying the subject matter" (Groomer, 2000). These definitions align with those of the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), which published a joint report in 1999 defining continuous auditing as "a methodology that enables independent auditors to provide written assurance on subject matter for which management is responsible, using a series of auditors' reports issued virtually simultaneously with, or shortly after, the occurrence of events underlying the subject matter" (AICPA/CICA Research Report, 1999).

Although the definitions provided by academics and professional organizations are very similar in meaning, the consensus among foreign experts on the definition of continuous auditing has not been matched by the corresponding development of appropriate methodologies. However, later North American academics and practitioners began to more clearly distinguish between continuous internal control technologies and auditing. For instance, Canadian author D. Coderre published an Institute of Internal Auditors standard in 2005 dedicated to continuous control. The document clearly differentiates between continuous internal control (performed by management and termed "monitoring") and continuous auditing itself (Coderre, 2005). D. Coderre understands continuous auditing quite broadly, as a process that "measures specific attributes that, if certain parameters are met, will trigger auditor-initiated actions". Warren and Parker similarly characterize continuous auditing, defining it as "a process that tests transactions based on pre-defined criteria, identifies anomalies, and for which the auditor is responsible..." (Warren & Parker, 2005).

However, among organizations surveyed about continuous auditing in North America, only 9 percent indicated its application across all major business components; 27 percent apply it in specific business processes. On the other hand, a large percentage of organizations (38%) plan to adopt this approach in the future, and only 20 percent neither use nor plan to use this methodology (New Demands, 2006).

Table. **Publication of Financial Statements on the Internet by Ukrainian Enterprises**

Does the enterprise publish its financial statements on the Internet for public use?	Total	Share, %
Yes	42	37.5
No	70	62.5
Total	112	100.0

Figure 1 presents a theoretical diagram illustrating how continuous control functions within enterprise computer information systems.

The continuous control system must constantly receive data from various sources and databases. Subsequently, data are verified using control technologies according to established norms and rules. Clear deviations requiring immediate attention are promptly reported to managers and financial analysts. Suspicious transactions are recorded, and subsequently, more sophisticated analytical models are applied to them to compare data against expected historical and statistical norms.

According to the theoretical framework, the implementation of continuous control involves the following sequential stages:

1. Identification of a control rule for each internal control point within a given business process area, following a generally accepted framework, such as COSO (www.coso.org).
2. Establishment of checks that apply each control rule through transaction analysis.
3. Establishment of checks to identify suspicious transactions based on patterns of anomalous operations.
4. Verification of all transactions on a regular and timely basis.
5. Identification of all transactions that failed the checks and notification of managers.
6. Investigation of each flagged transaction and appropriate response, followed by correction of the transaction where feasible.

Ideally, all suspicious transactions should be tracked by the software that records them – that is, corporate accounting and financial systems. Leung Chung Pak (1998) noted that "since checks need to be performed by external auditors continuously, audit software should be integrated with real-time operations." Indeed, a literature review reveals certain historical trends in building such control technologies (embedded control modules) within computer systems. Although embedded control modules can be seen as the primary precursor to continuous control technology, their development has been complex. Implementing embedded control modules proved difficult in many large organizations that had made significant investments in complex Enterprise Resource Planning (ERP) systems. Research found that support for embedded audit modules in the most common large ERP systems is extremely limited (Debreceny et al., 2003). Other US authors, based on surveys, also established that the limited support for embedded control modules is mainly due to a lack of user demand (despite developers claiming that embedded control modules are technically feasible) (Abdolmohammadi & Sharbatouglie, 2005).

Due to these implementation challenges, some authors (Vasarhelyi et al., 2002) suggest limiting the application of continuous auditing to areas encompassed by the enterprise's ERP systems. From this perspective, continuous control is viewed as an integral part of overall business automation.
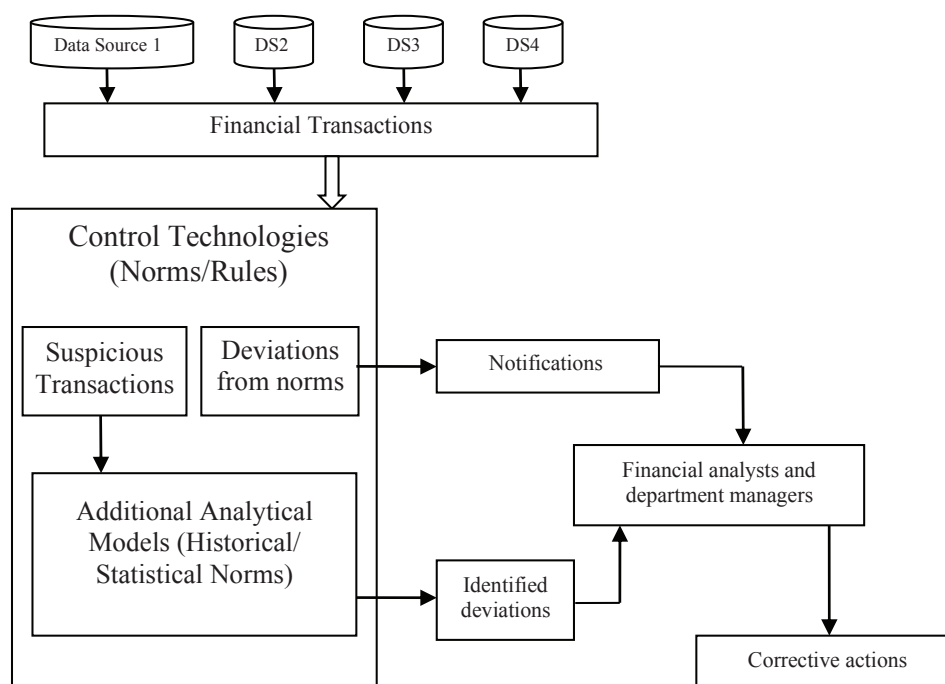

Fig. 1. Theoretical Scheme for Implementing Continuous Control

Effectively, continuous internal control is necessary for managers to ensure the proper implementation of their policies, procedures, and business processes. This process typically involves automated verification of all system transactions and activities within a specific business process, according to defined control rules (norms). Depending on the specific rules, corresponding checks, and threshold parameters, certain transactions are flagged as control exceptions and reported to management. For instance, a continuous control module embedded in the accounts payable subsystem might detect issues such as multiple monthly payments to the same supplier for invoices that should be consolidated into a single monthly payment, thereby saving time and costs.

In cases where managers exercise continuous control over business processes, auditors should avoid applying identical technologies. The challenge is that software procedures in ERP systems typically impact hundreds of other procedures, posing a high risk of disrupting core transaction processing systems when modifying any component. Instead, auditors should perform other procedures to determine if they can rely on the internal control process implemented by management.

M. Abdolmohammadi and A. Sharbatouglie (2005, p. 23) highlight another problem: modifying or replacing major subsystems of computer information systems to implement key internal controls is often impossible due to significant costs. Additionally, insufficient documentation for legacy systems poses another challenge in developing and implementing continuous control software modules.

An alternative to embedded control modules is a compromise approach in which transactions are periodically (e.g., nightly) extracted and transferred to a separate data warehouse, and subsequently analyzed using specialized audit software. Essentially, this approach allows both internal and external auditors to provide near-continuous assurance regarding information generated in computer business systems, largely independent of the effectiveness of manual or automated control technologies implemented by management. We propose referring to this form of enterprise control as a "periodic" audit (see Fig. 2).

According to the Cambridge Dictionary (dictionary.cambridge.org), "periodic" is defined as occurring repeatedly over a period of time. Similarly, Merriam-Webster (www.merriam-webster.com) defines "periodic" as occurring or recurring at regular intervals. Both definitions emphasize repetition and regular intervals in the meaning of "periodic."

We contend that the term "periodic audit" is most suitable for denoting a control technology in which data verification is genuinely periodic (rather than truly continuous) and subsequent (rather than preceding), yet the intervals between checks do not exceed one day, allowing managers to respond promptly to emerging issues.

The periodic audit approach theoretically contrasts with the concept of continuous reporting and continuous assurance of financial and other information for stakeholders. However, while participants in the study (auditors, financial analysts, CFOs) agree that monthly reporting is technically and economically feasible, they consider daily financial reporting currently impractical.

The following section examines the technologies for implementing and applying periodic audit in greater detail. Once data has been obtained, transformed, and stored in the audit data warehouse, auditors can perform analyses to detect reporting exceptions. Statistical analysis methods may include trend analysis (e.g., using moving averages), scatter plots for outlier detection, regression analysis to elucidate relationships between variables, cluster analysis, decision trees, and neural networks.

It is important to note that computer systems automating individual functions, such as accounting, collect and process their own data, often with considerable variations in data structure. These differences lead to incompatibility problems, complicating comparisons between reports. For example, while the marketing department might use a customer order as the critical event for revenue recognition, the production and accounting systems might use shipment as the critical event. For periodic audit purposes, a clear distinction should be maintained between data acquisition and subsequent analysis

Generally, the process of acquiring data for subsequent analysis in periodic audit should be organized into the following stages (Fig. 3):

1. Technologies for verifying, correcting, and loading operational data (including from various sources) into a unified database.
2. Technologies for querying data residing in the data warehouse.
3. Technologies for analyzing the acquired data.

Data analysis for management purposes may involve creative approaches; conversely, accumulating data for control purposes can yield erroneous results if a structured methodology is not applied. The primary objective of data analysis is to establish patterns within data and transactions, allowing unexpected items to serve as indicators for potential fraud. In such cases, audit software can
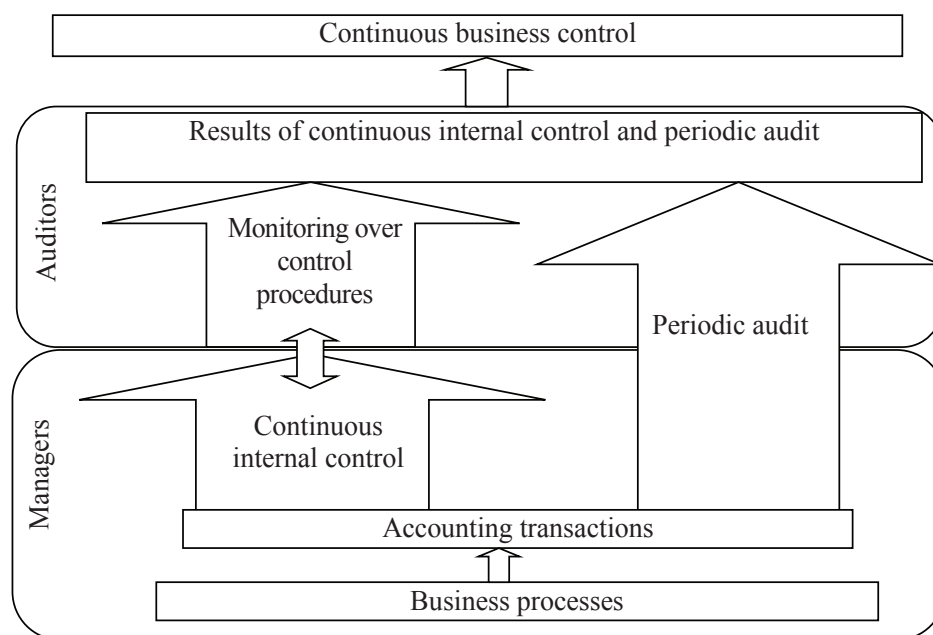
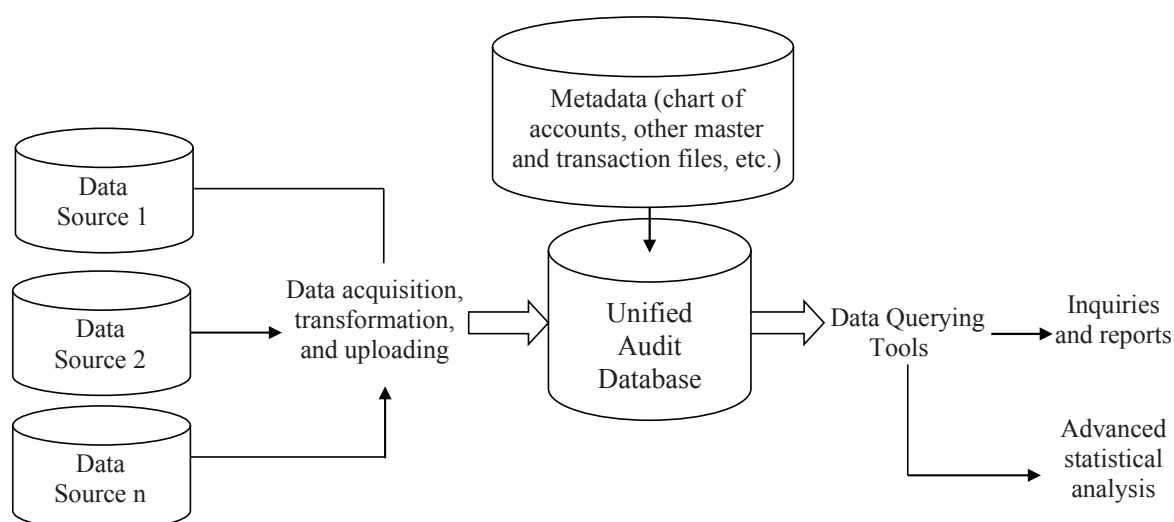**Fig. 2.** Conceptual Models of Continuous Internal Control and Periodic Audit

Fig. 3. General Model for Obtaining Data for Periodic Audit Purposes

detect specific anomalies, including missing or duplicate invoice numbers, or suppliers with similar names or other identifying details.

The proposed periodic audit model involves importing data from various sources and formats into a specially designed XML format. An enterprise might have an XBRL-based data warehouse. If so, existing XML data may only require minor modification, instead of being imported from legacy or real-time online systems.

Conclusions. We believe the concept of periodic audit is particularly beneficial in the context of Ukraine, where a generally low level of practice and culture regarding enterprise management is observed. In the future, tools for continuous control and auditing of financial transactions will become an integral part of accounting and financial systems. When suspicious situations arise, they will generate notifications about the problem's origin and allow tracing the entire processing path of the relevant transaction through files and networks. Subsequently, such accumulated statistical information can be analyzed to identify both individual problematic transactions and major trends and methods of fraud, as well as the most typical errors.

However, two important points should be noted. First, continuous internal control and periodic audit cannot be successful in detecting all exceptions.

Moreover, they can be significantly flawed. Since the rules for detecting exceptions are based on analytical studies, they have two drawbacks: they can fail to notice errors in some cases, and they can also trigger false positives. Failing to detect errors is a more serious drawback. For example, if a payment order to a shell company is not detected by the data retrieval system, perhaps because it failed to check the company's name against public data like bank or tax administration "blacklists," the consequence could be a significant financial loss. False positives, on the other hand, waste auditors' time and effort that could be used to track illicit activities. Sometimes, false positives can lead to customer loss. For example, if a bank blocks a customer's account after a cash deposit, citing the transaction's "unusualness," because all other deposits were non-cash. Indeed, a study (Bell et al., 2002) showed that automated continuous audit systems with 99%

reliability, if applied to all non-cash transfers in the US, would result in 400 false positives (flagged as illicit but actually legitimate) for every 20 actual money laundering cases detected (given the estimated rate of illicit transfers is only 0.05% of the total). Therefore, a drawback of continuous control and audit systems is that even with an extremely low transaction error rate, such systems will generate a number of warnings significantly exceeding the number of actual problems.

The proposed technology is versatile for identifying major internal control deficiencies in various conditions, enterprises, information systems, and different ways of organizing business and accounting. However, in any case, understanding business processes, preparing detailed flowcharts of the key activities being audited, and implementing appropriate internal control technologies are necessary.

References

Abdolmohammadi, M. J., & Sharbatouglie, A. (2005). *Continuous Auditing: An Operational Model for Internal Auditors*. Institute of Internal Auditors Research Foundation.

AICPA/CICA Research Report on Continuous Auditing. (1999). American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants.

Bell, T., Peecher, M. E., & Solomon, I. (2002). The Strategic-Systems Approach to Auditing. In T. B. Bell & I. Solomon (Eds.), *Cases in Strategic-Systems Auditing*. KPMG, LLP.

Coderre, D. (2005). *GTAG 3 – Global Technology Audit Guide. Continuous Auditing: Implications for assurance, monitoring, and risk assessment*. The Institute of Internal Auditors.

Debreceny, R., Gray, G. L., Tham, W. L., Goh, K. Y., & Tang, P. L. (2003). The Development of Embedded Audit Modules to Support Continuous Monitoring in the Electronic Commerce Environment. *International Journal of Auditing*, 7, 169–185.

Groomer, S. M. (2000). Continuous Audits: The Wave of the Future. *Charter*, *71*(1), 44–45.

Helms, G. L. (2002). Traditional and Emerging Methods of Electronic Assurance. *The CPA Journal*, *72*(3), 26–31.

Hunton, J. E., Wright, A., & Wright, S. (2002). *Assessing the Impact of More Frequent External Financial Statement Reporting and Independent Auditor Assurance on Quality of Earnings and Stock Market Effects*. Papers of the Fifth Continuous Auditing Symposium. Rutgers University.

Leung Chung Pak, W. (1998). *Concurrent auditing on computerized accounting systems (Thesis)*. University of Hong Kong.

New Demands, New Priorities. The Evolving Role of Internal Audit. Global Audit Executives Survey Report. (2006). ACL Services.

Vasarhelyi, M. A., Kogan, A., & Alles, M. A. (2002). Would Continuous Auditing Have Prevented the Enron Mess? *The CPA Journal, 72*(7), 80.

Warren, J. D., & Parker, X. L. (2003). *Continuous auditing: potential for internal auditors*. Institute of Internal Auditors Research Foundation.

Івахненков С. В.

РОЗРОБЛЕННЯ КОНЦЕПТУАЛЬНОЇ МЕТОДОЛОГІЇ ПЕРІОДИЧНОГО АУДИТУ ОБЛІКОВОЇ ІНФОРМАЦІЇ

Метою статті є розроблення методології безперервного контролю та аудиту фінансової та бухгалтерської інформації в умовах швидкого розвитку апаратних і програмних технологій, що уможливлюють електронну звітність у режимі реального часу. Описано сучасні технології, які можуть бути використані для безперервного аудиту та аналізу даних, зокрема для забезпечення достовірності інформації, що генерується інформаційними системами. Окремо розглянуто концепцію періодичного аудиту як альтернативу вбудованим модулям контролю, особливо актуальну для українських умов.

Методи дослідження. У статті проведено аналіз сучасних досліджень і публікацій щодо звітності в режимі реального часу та безперервного аудиту, зокрема праць американських і канадських дослідників та професійних організацій (Американського інституту сертифікованих громадських бухгалтерів (Association of International Certified Professional Accountants – AICPA), Канадського інституту дипломованих бухгалтерів (Canadian Institute of Chartered Accountants – CICA), Інституту внутрішніх аудиторів). Розглянуто теоретичні схеми реалізації безперервного контролю та концептуальні моделі періодичного аудиту. Проаналізовано стандарти електронної звітності, зокрема

XBRL, і практику їх впровадження у світі та, зокрема, в Україні. Описано технології отримання, перевірки, завантаження та аналізу даних для періодичного аудиту, зокрема статистичні методи (аналіз трендів, регресійний аналіз, кластерний аналіз та ін.). Також використано дані опитувань українських підприємств щодо публікації фінансової звітності в інтернеті.

Результати дослідження. Технології дають змогу створювати звітність у реальному часі, проте дослідження показує, що це потребує відповідного безперервного контролю та аудиту для забезпечення достовірності інформації. Традиційні підходи до безперервного аудиту, що передбачають вбудовані модулі контролю в ERP-системи, мають суттєві недоліки: ризики для стабільності системи, висока вартість впровадження та обмежена підтримка з боку розробників. Як альтернативу запропоновано концепцію періодичного аудиту. Цей підхід передбачає періодичне (наприклад, щоночі) вивантаження транзакцій в окреме сховище даних та їхній подальший аналіз за допомогою спеціалізованого аудиторського програмного забезпечення. Це дає змогу забезпечити майже безперервну впевненість щодо інформації незалежно від ефективності внутрішнього контролю підприємства. Запропоновано загальну модель отримання даних для періодичного аудиту, що має етапи перевірки, корекції, завантаження та аналізу даних. Визначено, що головною метою аналізу даних є виявлення несподіваних патернів, які можуть свідчити про шахрайство або помилки.

Можливе застосування результатів дослідження. Запропоновану методологію періодичного аудиту можуть застосовувати внутрішні та незалежні аудитори для забезпечення майже безперервної впевненості щодо достовірності фінансової та бухгалтерської інформації, що генерується комп'ютерними системами підприємств. Цей підхід є особливо корисним в умовах, коли рівень внутрішнього контролю є недостатнім, зокрема в Україні. Технологія є універсальною для виявлення суттєвих недоліків внутрішнього контролю в різних умовах, на різних підприємствах та в різних інформаційних системах. Результати можуть бути використані для вдосконалення практики аудиту, підвищення якості фінансової звітності та своєчасного виявлення шахрайства і помилок.

Висновки. Швидкий розвиток технологій вимагає переходу до безперервного або майже безперервного контролю фінансової інформації. Концепція періодичного аудиту, що передбачає регулярний аналіз даних, вивантажених в окреме сховище, є практичною та компромісною альтернативою вбудованим системам безперервного контролю, особливо в умовах обмежених ресурсів або недосконалих систем внутрішнього контролю. Цей підхід дає змогу аудиторам надавати своєчасну впевненість щодо даних із мінімальними затримками. Незважаючи на переваги, системи безперервного контролю та періодичного аудиту мають обмеження, зокрема ризик невиявлення помилок і генерації хибних спрацьовувань. Успішне впровадження потребує розуміння бізнес-процесів та адекватних технологій внутрішнього контролю. Концепція періодичного аудиту є особливо актуальною для України через потребу в підвищенні культури управління та контролю.

_____

Івахненков Сергій Володимирович – доктор економічних наук, професор кафедри фінансів Національного університету «Києво-Могилянська академія»

Sergiy Ivakhnenkov – Doctor of Economics, Professor of the Finance Department, National University of Kyiv-Mohyla Academy

https://orcid.org/0000-0001-7788-8659

ivakhnenkov@ukma.edu.ua