ECONOSCITECH INTEGRATION

ISSUE 7

INTERNATIONAL SCIENTIFIC ELECTRONIC JOURNAL

TASHKENT STATE UNIVERSITY OF ECONOMICS

American University of Technology
Powered by Arizona State University®

ISSN: 3060-5075

Acceptance of articles
PUBLISHED EVERY MONTHLY

ARTICLE CONTRIBUTORS
PROFESSORS-TEACHERS, SPECIALISTS AND SCIENTIFIC RESEARCHERS.

Google scholar

OpenAIRE

ISSN INTERNATIONAL STANDARD SERIAL NUMBER DENMARK

CONTACT: +998 94 3540880 https://econoscitech-integration-journal.uz

2026

THE SCIENTIFIC-POPULAR ELECTRONIC JOURNAL **"ECONOSCITECH-INTEGRATION"** HAS BEEN REGISTERED UNDER THE NUMBER C-5669651 BY THE AGENCY FOR INFORMATION AND MASS COMMUNICATIONS (AOKA) OF THE REPUBLIC OF UZBEKISTAN, EFFECTIVE FROM OCTOBER 9, 2024.

In accordance with Resolution No. 384/6 dated April 10, 2026, issued by the Presidium of the Supreme Attestation Commission under the Ministry of Higher Education, Science and Innovation of the Republic of Uzbekistan, this journal is included in the list of recommended international scientific publications for publishing the primary research findings of doctoral dissertations in the field of Economic Sciences.

Partners: Tashkent State University of Economics / American University of Technology in Tashkent (AUT)

Electronic publication. Issue 7. 374 pages.
Approved for publication in July 2026.

Editorial Board Members:

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

ORGANISATIONAL AND METHODOLOGICAL MECHANISM FOR IMPLEMENTING CONTINUOUS AUDIT TOOLS IN THE INTERNAL AUDIT OF COMMERCIAL BANKS

Ismailov Azizbek Madaminovich
Independent Researcher at Tashkent State University of Economics

Abstract. This article proposes an organisational and methodological mechanism for the gradual implementation of continuous audit tools in internal audit practice amid the digitalisation of banking services. The concept of continuous auditing is clearly distinguished from continuous monitoring and audit automation, and the conditions necessary to preserve internal audit independence are identified. The study substantiates a seven-layer architecture extending from source systems to management and escalation, a model structure for a library of automated control rules and indicators, and a three-horizon implementation roadmap progressing from data analytics to advanced analytics. The proposed mechanism is intended to address limitations in the audit coverage provided by traditional sample-based approaches and is integrated with risk-based planning within a unified management cycle. The study also identifies the principal implementation risks and proposes a system of performance indicators for evaluating the effectiveness of continuous auditing.

Keywords: internal audit, commercial bank, continuous auditing, continuous monitoring, automated control indicators, data analytics, audit coverage, seven-layer architecture, control rule library, three-horizon roadmap.

Аннотация. В статье предложен организационно-методический механизм поэтапного внедрения инструментов непрерывного аудита в практику внутреннего аудита в условиях цифровизации банковских услуг. Понятие непрерывного аудита чётко разграничено с непрерывным мониторингом и автоматизацией аудита, а также определены условия, необходимые для сохранения независимости внутреннего аудита. Обоснованы семиуровневая архитектура, охватывающая этапы от исходных информационных систем до управления и эскалации, типовая структура библиотеки автоматизированных контрольных правил и индикаторов, а также трёхэтапная дорожная карта внедрения — от анализа данных до продвинутой аналитики. Предлагаемый механизм направлен на устранение ограничений охвата аудита, присущих традиционным выборочным подходам, и интегрирован с риск-ориентированным планированием в рамках единого управленческого цикла. В исследовании также определены основные риски внедрения и предложена система показателей эффективности непрерывного аудита.

Ключевые слова: внутренний аудит, коммерческий банк, непрерывный аудит, непрерывный мониторинг, автоматизированные контрольные индикаторы, анализ данных, охват аудита, семиуровневая архитектура, библиотека контрольных правил, трёхэтапная дорожная карта.

INTRODUCTION

The rapid digitalisation of banking services presents a fundamental challenge for internal audit. Traditional sample-based auditing, regardless of the quality of sample selection, covers only a limited proportion of the continuously increasing volume of banking transactions. Consequently, errors and control deficiencies may be identified only after they have occurred and, in some cases, after a significant period has elapsed. These limitations in audit coverage cannot be addressed solely through improvements in audit planning; they also require the technological enhancement of audit-evidence collection processes.

The relevant international standards support this direction. The Global Internal Audit Standards require the chief audit executive to regularly assess opportunities to use technological resources to improve the effectiveness and efficiency of the internal audit function [4]. The first Topical Requirement adopted by The Institute of Internal Auditors specifically addresses cybersecurity [5]. At the same time, national regulatory requirements do not yet provide detailed guidance on the application of data analytics and continuous audit tools [2]. As a result, the development of this technological area largely depends on banks' own initiatives and the availability of appropriate methodological support.

The concept of continuous auditing is not new. Its conceptual foundations emerged in the 1990s in response to the challenges associated with auditing online information systems [7]. For a considerable period, its broader implementation was constrained by two major factors: limited real-time access to data and insufficient computing capacity. Digital transformation has substantially reduced both constraints. Therefore, the current methodological question is no longer whether continuous auditing can be implemented, but how it should be implemented effectively while preserving internal audit independence and professional judgement.

The purpose of this article is to develop and substantiate an organisational and methodological mechanism for the gradual implementation of continuous audit tools—including automated control indicators, data analytics, and continuous audit procedures—in the internal audit practice of commercial banks. To achieve this purpose, the study distinguishes continuous auditing from related concepts, develops a seven-layer architecture, proposes a model structure for a control rule library, establishes a three-horizon implementation roadmap, and identifies the principal implementation risks and performance indicators.

LITERATURE REVIEW

The academic foundations of continuous auditing were established by M. A. Vasarhelyi and F. B. Halper in their study of the continuous auditing of online systems. The authors advanced the idea that audit evidence could be collected automatically at the time transactions occur or shortly thereafter [7]. The technological guidance issued by The Institute of Internal Auditors subsequently systematised the continuous assurance approach by explaining the coordination of continuous auditing and continuous monitoring [6]. The Global Internal Audit Standards establish the effective use of technology as a responsibility of the chief audit executive [4], while the Cybersecurity Topical Requirement establishes minimum expectations for auditing high-risk digital activities [5].

Within the banking context, the Basel Committee on Banking Supervision emphasises the need for comprehensive audit coverage [8]. The Three Lines Model assigns continuous monitoring primarily to management and second-line functions, while continuous auditing remains an independent third-line activity [10]. In Uzbekistan, the Regulation on Requirements for Risk Management Systems of Banks and Banking Groups, registered under No. 3427, provides the regulatory basis for establishing risk management and management monitoring systems [3]. The COSO frameworks similarly identify monitoring as an integral component of an effective internal control system [9].

In the national academic literature, issues relating to the organisation of internal audit in accordance with international standards have been examined in the works of A. K. Ibragimov [11], N. F. Karimov [12], G‘. D. Tashmanov [13], and N. Sh. Khajimuratov [14].

Nevertheless, the existing literature primarily discusses continuous auditing at the conceptual level. A comprehensive organisational and methodological mechanism adapted to the practices of commercial banks in Uzbekistan—incorporating a clear distinction between continuous auditing, continuous monitoring, and automation; a layered architecture; a control rule library; and a gradual implementation procedure—has not yet been sufficiently developed. This article is intended to contribute to addressing this methodological gap.

RESEARCH METHODOLOGY

The study employed comparative conceptual delimitation, layered modelling, systems analysis, and logical generalisation. Three fundamental principles were established in designing the proposed mechanism.

The first principle is independence: continuous audit tools should be owned and controlled by the internal audit function, while management access should be organised in a manner that prevents any alteration of audit results.

The second principle is gradualism and proportionality: implementation should proceed through successive horizons corresponding to the bank’s size, technological maturity, and organisational readiness, without omitting any implementation stage.

The third principle is integration: the mechanism should not operate as an isolated warning system but should be designed as an integral part of the audit cycle, closely linked to risk-based planning, audit engagements, and the monitoring of recommendations.

The information base of the study comprised the Global Internal Audit Standards, topical requirements, technological guidance, and position papers issued by The Institute of Internal Auditors [4–6; 10], documents of the Basel Committee on Banking Supervision [8], the COSO conceptual frameworks [9], and the fundamental academic literature on continuous auditing [7].

The national regulatory framework included the Law of the Republic of Uzbekistan No. ZRU-580 “On Banks and Banking Activities” dated November 5, 2019 [1]; the Regulation on Requirements for Internal Audit

in Commercial Banks, approved by Resolution No. 3/2 of the Board of the Central Bank of the Republic of Uzbekistan dated April 16, 2021, and registered by the Ministry of Justice under No. 3302 on May 7, 2021 [2]; and the Regulation on Requirements for Risk Management Systems of Banks and Banking Groups, approved by Resolution No. 4/11 of the Board of the Central Bank dated March 7, 2023, and registered by the Ministry of Justice under No. 3427 on April 18, 2023 [3].

The proposed solutions were designed with due consideration of the specific characteristics of banking processes and the resource capacity of internal audit functions.

ANALYSIS AND RESULTS

The analysis begins with a clear definition of continuous auditing because, in practice, it is frequently confused with either audit automation or continuous monitoring. Continuous auditing is a process controlled by the internal audit function through which audit evidence is collected and evaluated automatically at the time transactions occur or shortly thereafter [7]. It is important to distinguish continuous auditing from two related concepts (Table 1). Continuous monitoring is a management function that continuously observes the operation of controls and generally belongs to management and second-line functions. Continuous auditing, by contrast, is an independent third-line activity that evaluates both the underlying controls and the effectiveness of management's monitoring system [6; 10].

Continuous auditing also differs from basic audit automation. Merely converting individual audit procedures into software-based processes does not make an audit continuous. Continuity requires the repeated and scheduled execution of audit tests, the systematic evaluation of exceptions, and the application of professional auditor judgement to the resulting evidence.

Table 1
Comparison of Continuous Auditing, Continuous Monitoring, and Audit Automation

Criterion	Continuous Auditing (CA)	Continuous Monitoring (CM)	Audit Automation
Responsible entity	Internal audit function (third line)	Management and second-line functions	Internal audit function
Purpose	Provision of independent assurance through the assessment of controls and monitoring systems	Ensuring the continuous and effective operation of controls	Improving the efficiency of audit procedures
Frequency	Repeated at scheduled intervals or performed in near real time	Continuous or near real time	Performed within individual audit engagements, usually on a one-off basis
Coverage	Full population (100%)	Entire monitored population	Sample-based or full-population analysis
Independence	Independent; the tools are governed and overseen by the internal audit function	Not independent; it forms part of management's control activities	Depends on the governance of the tools; automation alone does not ensure continuity

Source: developed by the author.

The relationship between continuous auditing and internal audit independence is a fundamental methodological consideration. Excessive reliance on management's continuous monitoring system may limit the ability of internal audit to provide an independent assessment of control effectiveness. Therefore, a two-level approach is appropriate: the internal audit function should assess the design and operating effectiveness of management monitoring while maintaining its own continuous audit indicators based on independent assessment criteria. This approach enables internal audit to identify risks that may not be detected through management monitoring and enhances the reliability of assurance activities.

The proposed continuous audit architecture is based on a seven-layer model. The first layer comprises source systems, including automated banking systems, payment gateways, lending systems, human resources systems, and accounting systems. The second layer covers data collection and quality control: the internal audit function connects to the relevant systems in read-only mode, retrieves data according to a predefined schedule, and assesses their completeness, integrity, consistency, and accuracy. Data that do not satisfy the established quality requirements are not transferred to the rule-processing stage. The third layer comprises a library of control rules and tests consisting of algorithms designed to address specific risks and examine the entire data population. The fourth layer consists of continuous risk indicators that identify changes in the level of risk. The

fifth layer comprises continuous control indicators that assess whether the relevant control mechanisms are operating effectively. The sixth layer covers analysis and classification, under which exceptions are prioritised according to their significance and low-relevance alerts are filtered. The seventh layer comprises management and escalation procedures: significant exceptions are referred to the responsible auditor and, where appropriate, to the audit committee, while aggregated indicators are presented on a dashboard. Feedback is maintained across the layers, allowing newly identified risks to be incorporated into the control rule library [6; 9].

The fourth and fifth layers—risk and control indicators—represent two distinct but complementary dimensions of continuous auditing. Risk indicators determine whether the level of risk has increased by monitoring process outcomes, such as rejection rates, overdue payments, and the frequency of unusual transactions. Control indicators assess whether the relevant control mechanisms are operating effectively by examining, for example, whether transactions exceeding established limits have received appropriate approval and whether the segregation of duties has been maintained. Their combined application provides a comprehensive diagnostic framework. An increase in risk accompanied by control deficiencies indicates the need for prompt review, whereas a low level of observed risk combined with control deficiencies indicates a latent weakness in the control environment. In the latter case, no adverse consequence may yet have occurred, although the relevant control mechanism is not operating effectively. This two-dimensional assessment provides a level of diagnostic detail that may be difficult to achieve through traditional sample-based auditing alone.

The third layer—the control rule library—constitutes the operational core of the architecture (Table 2). A standardised record is maintained for each rule, specifying the risk addressed, the rule logic, execution frequency, exception threshold, and responsible auditor. The library is maintained as a continuously updated methodological resource: new rules are introduced as emerging risks are identified, ineffective rules are reviewed, and the operational effectiveness of each rule is periodically assessed by examining the number of times it was triggered, the proportion of confirmed exceptions, and the frequency of low-relevance alerts. All changes are subject to version control. An effective rule should possess four characteristics: specificity, meaning that it addresses a clearly defined risk; scalability, meaning that it can be applied using available data fields; proportionality, meaning that the exception threshold identifies significant issues without generating an excessive number of low-relevance alerts; and actionability, meaning that each identified exception results in a defined response, such as further examination, corrective action, or escalation.

Table 2
Illustrative Content of a Continuous Audit Control Rule Library

Process	Examples of Control Rules and Indicators	Risks Addressed
Credit transactions	Loans exceeding established limits or approval authority; loan agreements with incomplete supporting documentation; lending to related parties exceeding approved limits; inconsistencies between loan classification and provisioning	Credit risk, unauthorised activity, inadequate provisioning
Payment and operational activities	Large-value transactions conducted outside normal working hours; split or structured payments; cancelled and re-entered transactions; duplicate payments	Fraud risk, money laundering risk, operational error
Authorisation and access rights	Violations of the segregation of duties; active user accounts assigned to former or inactive employees; inappropriate or inconsistent access rights	Operational risk, cybersecurity risk
Deposits and commissions	Unusual interest rates; incorrectly calculated commissions; unusual movements in large deposits	Revenue loss, customer protection risk, liquidity risk
Reporting and system settings	Manual changes to system reference data; changes to key system parameters; inconsistencies between accounts	Risk to the reliability of financial reporting

Source: developed by the author.

Implementing the entire architecture simultaneously may be impractical and may increase implementation risk. Accordingly, the architecture should be introduced gradually, taking into account the bank's technological capacity, organisational readiness, and available resources. For this purpose, a three-horizon implementation roadmap is proposed (Table 3).

INTERNATIONAL SCIENTIFIC ELECTRONIC JOURNAL

Particular attention should be given to the first horizon, as it represents the most accessible initial stage of implementation but is often insufficiently prioritised. Continuous auditing is sometimes regarded as requiring the immediate acquisition of specialised software, which may lead institutions to postpone its introduction. However, the first horizon can be implemented without specialised technological solutions. Full-population analysis may initially be conducted using spreadsheet applications and basic database queries.

At this stage, the principal requirement is the development of auditors' data-analysis competencies rather than substantial investment in technology. The first horizon provides two important benefits: it enables an immediate expansion of audit coverage and establishes the foundations required for the subsequent horizon, including validated control rules, trained personnel, and reliable data flows.

Table 3
Three-Horizon Roadmap for Implementing Continuous Audit Tools

Horizon	Content	Implementation Requirements and Conditions for Progression
Horizon 1. Data Analytics	Full-population analysis using spreadsheet software and database query tools; development of a library of repeatable audit tests; regular preparation of exception reports through partially manual procedures	A set of validated and stable rules; automated extraction of structured data; an established exception-management process
Horizon 2. Automated Continuous Audit Testing	Automated execution of audit tests according to a predefined schedule; implementation of an exception dashboard and alert system; integration of results with the recommendation-tracking register	A sufficient volume of reliable historical data; appropriate internal expertise or access to external specialists; stable operation of scheduled automated testing
Horizon 3. Advanced Analytics	Automated anomaly detection, including selected machine-learning techniques; analysis of textual data; development and application of predictive risk indicators	Validated analytical models; adequate data quality; documented and explainable model logic; effective auditor oversight and professional judgement

Source: developed by the author.

Each horizon builds on the knowledge, experience, and capabilities developed during the preceding stage. The pace of transition should be proportionate to the bank's size, technological maturity, organisational readiness, and available resources. Smaller banks may remain within the first horizon for a longer period, whereas larger and more technologically advanced banks may progress more rapidly to the second and third horizons. Completion of the principal requirements of each stage before proceeding to the next supports the stability and effectiveness of subsequent implementation.

The same principle applies to the selection of technological tools. Rather than giving priority to the most advanced available solution, banks should select tools that correspond to their current level of readiness and operational requirements. The main selection criteria should include compatibility with existing information systems, ease of use and adoption by auditors, and the transparency and explainability of the underlying rule logic.

The relationship between the proposed mechanism and risk-based planning is reciprocal, which enables continuous auditing to function as an integral part of the audit system rather than as a separate analytical tool. On the one hand, continuous indicators provide inputs to the planning trigger mechanism. The activation of an indicator may lead to the reassessment of the relevant auditable entity or area and, where necessary, revision of the audit plan. On the other hand, risk-based planning determines the order in which continuous audit rules are developed and applied, with higher-risk auditable entities or areas receiving priority.

Identified exceptions are incorporated into the audit cycle through three principal procedures. Minor and isolated exceptions are referred to the responsible department for review and corrective action. Recurring or systemic exceptions may result in the initiation of a thematic audit engagement. Exceptions involving significant financial amounts or indications of potential fraud are subject to prompt escalation in accordance with established procedures. All identified exceptions and the measures taken in response are recorded in a centralised register.

The relationship between continuous auditing and IT auditing should also be clearly defined. Continuous auditing is an audit method based on the repeated or automated assessment of transactions and controls, whereas IT auditing concerns the examination of information systems, technology governance, cybersecurity,

and related controls. The two areas are complementary. Where specialised expertise is limited, the IT audit component may be introduced through a co-sourcing arrangement. Under this arrangement, the bank's internal audit function retains responsibility for planning and managing the engagement, evaluating the evidence, and approving the results, while external specialists provide the required technical expertise.

The practical risks associated with implementation should be considered from the outset. The first risk is a high volume of false-positive alerts. An excessively sensitive rule may generate numerous low-relevance alerts and reduce the efficiency of exception analysis. This risk can be addressed through pilot testing, periodic review of rule performance, and calibration of exception thresholds.

The second risk concerns insufficient algorithmic transparency. When the logic underlying a complex analytical model cannot be adequately explained, the reliability and practical usefulness of its results may be questioned. Accordingly, rule logic, input data, assumptions, and decision criteria should be clearly documented and made understandable to the responsible auditors.

The third risk is excessive reliance on technological outputs. Continuous auditing should not replace professional judgement; rather, it should provide additional evidence to support the auditor's assessment and decision-making.

The fourth risk relates to internal audit independence. The continuous audit tools should remain under the governance and oversight of the internal audit function. Access rights should be clearly defined, all changes to rules and parameters should be recorded, and the integrity of data and analytical results should be protected through appropriate technical and organisational controls.

The effectiveness of the mechanism should be assessed through a system of measurable indicators. These may include the proportion of transactions covered by full-population analysis, the reduction in the time required to identify errors and control deficiencies, the number of automatically detected exceptions, the proportion of confirmed exceptions, and the number of audit-plan revisions resulting from continuous audit indicators.

CONCLUSIONS AND RECOMMENDATIONS

The findings of the study support the following conclusions.

First, in the context of digitalisation, the limitations in audit coverage associated with traditional sample-based auditing cannot be addressed solely through improvements in audit planning. They also require the technological enhancement of audit-evidence collection and analysis. Continuous auditing should be clearly distinguished from continuous monitoring and audit automation. In addition, the governance of continuous audit tools should remain with the internal audit function, while the two-level approach—comprising the assessment of management monitoring and the use of independent audit indicators—should be applied to preserve internal audit independence.

Second, the proposed seven-layer architecture—comprising source systems, data collection and quality control, the control rule library, risk indicators, control indicators, analysis and classification, and management and escalation—provides a structured basis for integrating continuous auditing into internal audit activities. The combined use of risk and control indicators enables a multidimensional assessment that may be difficult to achieve through traditional sample-based auditing alone. The feedback mechanism also allows the control rule library to preserve and accumulate the methodological knowledge of the internal audit function.

Third, the three-horizon roadmap—data analytics, automated continuous audit testing, and advanced analytics—allows implementation to be aligned with the bank's level of readiness. The first horizon may be implemented using existing technological tools and can expand audit coverage while developing the competencies, validated rules, and reliable data flows required for subsequent stages. Clearly defined transition criteria reduce the risk of premature progression between implementation stages.

Fourth, the proposed mechanism is integrated with risk-based planning within a unified audit-management cycle. Continuous audit indicators provide information for reassessing auditable entities or areas and revising the audit plan, while risk-based planning determines the priority of the rules to be developed and applied. Identified exceptions are incorporated into the audit process through corrective action, thematic audit engagements, or escalation, depending on their significance. The mechanism's effectiveness can be evaluated through indicators relating to audit coverage, detection time, exception-confirmation rates, and audit-plan revisions.

Based on these conclusions, the following recommendations are proposed: banks should begin implementation from the first horizon by applying full-population analysis through available technological tools and by prioritising the development of auditors' data-analysis competencies; the control rule library should be maintained as a continuously updated methodological resource supported by standardised rule records, performance statistics, and version control; internal regulations should clearly define the governance of audit tools, access restrictions, change-management procedures, and controls over the integrity of results;

professional associations should support the development of standard rule-library models and specialised training programmes; and regulatory authorities should consider developing methodological guidance on the use of continuous audit technologies.

These measures may contribute to addressing the existing methodological limitations in national regulation. The proposed mechanism is also closely related to the internal audit quality assurance and improvement programme and the performance-indicator system and provides a basis for further research.

REFERENCES

1. Republic of Uzbekistan. On Banks and Banking Activities: Law of the Republic of Uzbekistan No. ZRU-580 dated November 5, 2019 // National Database of Legislation of the Republic of Uzbekistan. — 2019. — November 6. — No. 03/19/580/4014. https://lex.uz/ru/docs/4581971
2. Board of the Central Bank of the Republic of Uzbekistan. On Approval of the Regulation on Requirements for Internal Audit in Commercial Banks: Resolution No. 3/2 dated April 16, 2021; registered by the Ministry of Justice of the Republic of Uzbekistan on May 7, 2021 under No. 3302 // National Database of Legislation of the Republic of Uzbekistan. — 2021. — May 7. — No. 10/21/3302/0486. https://lex.uz/uz/docs/-5431666
3. Board of the Central Bank of the Republic of Uzbekistan. *On Approval of the Regulation on Requirements for the Risk Management Systems of Banks and Banking Groups*: Resolution No. 4/11 dated 7 March 2023; registered by the Ministry of Justice of the Republic of Uzbekistan on 18 April 2023 under No. 3427, as amended. // National Database of Legislation of the Republic of Uzbekistan. — 19 April 2023. — No. 10/23/3427/0218. https://lex.uz/docs/-7335794
4. The Institute of Internal Auditors. Global Internal Audit Standards. — Lake Mary, FL: The Institute of Internal Auditors, 2024. — Issued January 9, 2024; effective January 9, 2025.
5. The Institute of Internal Auditors. Cybersecurity Topical Requirement. — Lake Mary, FL: The Institute of Internal Auditors, 2025. — Issued February 5, 2025; effective February 5, 2026.
6. The Institute of Internal Auditors. Continuous Auditing and Monitoring. — 3rd ed. — Lake Mary, FL: The Institute of Internal Auditors, 2025. — Global Technology Audit Guide.
7. Vasarhelyi, M. A.; Halper, F. B. The Continuous Audit of Online Systems // Auditing: A Journal of Practice & Theory. — 1991. — Vol. 10, No. 1. — P. 110–125.
8. Basel Committee on Banking Supervision. The Internal Audit Function in Banks. — Basel: Bank for International Settlements, 2012.
9. Committee of Sponsoring Organizations of the Treadway Commission. Internal Control—Integrated Framework. — New York: American Institute of Certified Public Accountants, 2013; Enterprise Risk Management—Integrating with Strategy and Performance. — New York: American Institute of Certified Public Accountants, 2017.
10. The Institute of Internal Auditors. Three Lines Model: Assurance and Advice in Support of Effective Governance: Statement of Position. — Lake Mary, FL: The Institute of Internal Auditors, 2026.
11. Ibragimov, A. K. Organizational Foundations of Internal Audit in Commercial Banks Based on International Auditing Standards: Textbook. — Tashkent, 2013. — 383 p. — ISBN 978-9943-302-80-8. — [In Uzbek].
12. Karimov, N. F. Internal Audit in Commercial Banks: Monograph. — Tashkent: Fan, 2006. — 262 p. — ISBN 5-648-03389-3. — [In Uzbek].
13. Tashmanov, G. D. Improving the Internal Audit Service Based on International Standards: Abstract of the Dissertation for the Degree of Doctor of Philosophy (PhD) in Economics. — Tashkent: Tashkent Institute of Finance, 2021. — 56 p. — [In Uzbek].
14. Khajimuratov, N. Sh. Improving the Methodology of Financial Statement Auditing: Abstract of the Dissertation for the Degree of Doctor of Science (DSc) in Economics. — Tashkent, 2021. — 36 p. — [In Uzbek].

Proofreader: Xondamir Ismoilov

Layout and Designer: Hasan Maqsudov

2026. № 7

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

Our address: Tashkent city, Yunusobod district, 19th block, House 17.