DOI: 10.55643/fcaptp.4.69.2026.5290

EVOLUTION OF INTERNAL AUDIT FOR ENHANCING IT COMPANIES' EFFICIENCY AMIDST DIGITAL TRANSFORMATION

Artem Basin
PhD Student, Department of Audit, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine;
ORCID: 0009-0003-4579-3315

Olena Petryk
D.Sc. in Economics, Professor of the Department of Audit, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine;
e-mail: auditlena@ukr.net
ORCID: 0000-0003-1881-9412
(Corresponding author)

Iryna Matiienko-Zubenko
Candidate of Economic Sciences, Associate Professor of the Department of Audit, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine;
ORCID: 0000-0003-0266-1489

Nataliia Kuzyk
Candidate of Economic Sciences, Associate Professor of the Department of Accounting and Taxation, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine;
ORCID: 0000-0001-5042-8759

Liudmyla Melnyk
D.Sc. in Economics, Professor of the Department of Accounting and Taxation, Uman National University, Uman, Ukraine;
ORCID: 0000-0003-2498-5556

Received: 03/07/2026
Accepted: 19/08/2026
Published: 31/08/2026

ABSTRACT

The object of this study is the internal audit system of IT companies in the environment of digital transformation and European integration. The main problem of auditing IT companies is the critical inefficiency of conventional and retrospective approaches in the case of fast automated transactions, complicated multi-component revenue recognition arrangements, and cloud-based ERP systems.

The goal of the research is to synthesize existing maturity models and to coordinate internal audit processes with the requirements of European regulations, namely: Corporate Sustainability Reporting Directive (CSRD), EU Artificial Intelligence Act (EU AI Act), and IFRS 15. Also, the internal regulation of the legal regime of "Diya City" in Ukraine is taken into consideration. Methodologically, the study employs historical-logical, comparative, and systematic analyses for the evaluation of existing paradigms and the creation of a structural analytic framework.

The main results of the study are a five-stage evolutionary model of internal audit maturity, which evolves from a reactive baseline paradigm to a predictive paradigm with the use of artificial intelligence. Modeling of the stages resulted in the creation of "Audit Layer" and "Compliance as Code" architecture. The financial control requirements are implemented as automated checks in DevOps and CI/CD pipelines in accordance with the proposed architecture. As a result, the audit paradigm shifted from ex-post error detection to ex-ante prediction of errors with autonomous blocking of incorrect financial transactions, including incorrect transaction price allocation. Also, a RACI matrix and adjusted KPI system are elaborated for audit performance assessment.

The main findings show that the combination of algorithmic blocking and behavioral monitoring with the use of AI closes the gap between IT and financial departments of a company. It is important for scaling up IT companies in the European digital market. Besides, the economic feasibility of moving to the advanced analytical stages is proven with the calculation of ROI ≥ 1.5 that considers financial risks of regulatory non-compliance.

Keywords: internal audit, IT companies, digital transformation, Compliance as Code, continuous auditing, maturity model, audit effectiveness, operational efficiency, automated control, European integration

JEL Classification: M41, M42, F15, L86

INTRODUCTION

The receipt of candidate status for Ukraine in 2022, together with ongoing negotiations in the Financial Services cluster, creates an entirely new regulatory environment for the Ukrainian information technologies sector. The process of European integration means that the EU standards for reporting, auditing, and compliance will turn from being only guidelines into musts for working in the unified European digital market. In addition to that, the CSRD (Corporate Sustainability Reporting Directive, 2024), EU AI Act (EU Artificial Intelligence Act, 2024), and the updated International Internal Audit Standards of the IIA (2024) are an important path for Ukrainian IT companies to enter the EU market.

The IT industry can be considered one of the key drivers of the digital economy of Ukraine, being the biggest export component in terms of the country's economic relationship with the European Union. According to DOU.ua, as of January 2026, the IT industry comprised over 303,000 specialists, with the export revenue from the sales of IT services amounting to USD 6.66 billion in 2025, accounting for 41.6% of the total value of service exports (DOU.ua, 2025). A significant part of these exports is supplied to the EU market, thus making these organizations subject to regulation in accordance with the Corporate Sustainability Reporting Directive (CSRD) and the EU Artificial Intelligence Act. Given the dynamics of development, IT companies are marked by the prevalence of intangible assets and complex service models, such as SaaS, PaaS, and pay-per-use. Classification of IT businesses into product-oriented, service-oriented, and mixed variants presupposes completely different approaches to organizing accounting procedures. The provision of reliable accounting reports serves as a basis for sustainable development of the IT industry, thus making internal auditing go beyond its control scope and become the means of boosting macroeconomic competitiveness on the European market.

Integration of Ukraine into the European community highlights already existing operational differences through its strict regulatory components. For entities operating within the sphere of information technology to be granted access to the European Union market, they are to provide documentation regarding their accounting approaches that would enable them to meet the CSRD requirements and ESRS standards. As a result, internal auditing becomes the means of obtaining access to the market. Papinko highlighted this specific issue with special focus on the use of IFRS 15 with respect to multi-element arrangements. Post-implementation analysis has shown that the same pattern emerges repeatedly: the IT sector raises the most difficult practical issues with regard to transaction price allocation and variable consideration.

The domestic regulatory setting needs special consideration in its process of harmonization in line with EU legislation. Adopted in 2021, the "Diia.City" legislation framework significantly changed the taxation process, labor laws, and the regulation of intellectual property rights for Ukrainian information-technology companies. The change impacts the accounting process and expenses in relation to gig workers and contractors. Within Chapter 4 of the legislation screening process ("Free Movement of Capital") conducted by the European Commission, the importance of transparent labor relations in the digital economy was emphasized. This requirement coincides with the audit of payments in accordance with the "Diia.City" legislation. As per the information from Opendatabot, as of early 2026, there were more than 3,700 companies with resident status, of which 2,844 companies belonged to the IT sector. Currently adopted laws and international standards of auditing (ISAs) set up a broad regulatory framework. However, they fail to cover the particular economic conditions of the IT sector.

These conditions make retrospective sampling obsolete. Rapid automated transactions create immediate systemic risks. Financial logic now lives directly inside billing algorithms or cloud ERP systems. Traditional control measures simply cannot mitigate these embedded threats. This reveals the primary research problem: the industry lacks a specific audit model that integrates financial control with digital development while aligning with key regulatory frameworks (CSRD, EU AI Act, updated IIA Global Standards). This study investigates IT internal audit systems navigating both digital transformation and European integration.

LITERATURE REVIEW

The transformation of internal audit under the dual pressure of digitalization and European integration has generated a growing body of scholarly and professional literature. To delineate the position of the proposed model within this body of knowledge and to substantiate the research gap it addresses, a systematic comparative analysis of key scientific, professional, and normative sources was conducted (Table 1). While the analysis of relevant literature is conducted globally, specific attention is given to the Ukrainian context of digitalization. The sources are grouped by research area and evaluated against two dimensions:

1. Their principal contributions to accounting and internal audit theory.
2. The limitations or gaps they leave unresolved.

DOI: 10.55643/fcaptp.4.69.2026.5290

Table 1. Key contributions and research gaps in IT internal audit literature (2022–2026).

№	Research Area	Authors and Year	Key Conclusions for Accounting/Internal Audit	Limitations and Research Gaps
1	The Ukrainian Context of Digitalization in Accounting and Auditing	Kononenko (2024); Lviv IT Cluster, 2026; Digital Transformation of Accounting and Auditing in Ukraine (2025)	Analyzes the impact of digital technologies, AI, and cloud services on the modernization of accounting processes and internal audit in Ukraine.	Describes digitalization primarily at the macroeconomic level, without developing sector-specific phased models tailored to the IT business and the specifics of SaaS.
2	Global Internal Audit Standards	The Institute of Internal Auditors (2024); PwC (2024)	Develops an updated global framework (Global Standards) that places greater emphasis on risk-based approaches, IT competencies, and the role of audit as the "third line of defense."	Provides general requirements but does not include specific industry-specific audit procedures for cloud-based ERP systems or development environments (DevOps).
3	Regulatory Practice (IFRS 15 in IT)	EFRAG (2024); IFRS Foundation (2024)	Based on the results of a post-implementation review, it is noted that software companies generate the largest share of systemic issues (multi-component transactions).	The documents are regulatory reports, not a methodology for organizing internal controls to detect such errors in real time.
4	Audit Maturity Models	KPMG International (2024); Clearsulting (2024)	Proposes levels of evolution of the audit function from a traditional approach to data analytics and fully automated oversight.	The models are industry-neutral; they do not account for the specifics of the evolution of revenue recognition rules (IFRS 15) and intangible assets (IAS 38) in the IT sector.
5	AI and Continuous Auditing	Wassie & Lakatos (2024); Fırat (2025)	The transition to Continuous Auditing is justified, as it has been shown that machine learning algorithms dramatically improve risk assessment.	Focuses on general financial landscapes without considering the integration of auditing into software development cycles (CI/CD) and billing systems.
6	IT Risks and Cybersecurity in Auditing	Protiviti & The Institute of Internal Auditors, 2023; SafePaaS (2025)	Analyzes the evolution of technology risks (cloud, AI, cybersecurity) as priorities for internal auditors.	Focuses on IT controls and security rather than on the impact of these risks on the reliability of accounting and financial reporting.
7	Accounting for Intangible Assets and Intellectual Capital	Papinko (2024); Shukurova & Plevako (2020)	Authors expose the unique asset structure of modern IT firms. They demonstrate how intangible assets and intellectual capital completely dominate the balance sheet. This structural shift creates severe, highly specific transformation risks.	Internal auditing only plays an indirect, background role in these studies. The literature lacks a concrete, actionable model to help digital auditors manage this highly "intellectualized" asset base.
8	Evolution toward ESG reporting	Hecimovic & Canestrari-Soh (2025)	Demonstrates the need to expand the internal audit mandates to include the assessment of non-financial information (ESG) and the sustainability of business models.	Considers ESG in isolation from the financial control of digital assets and monetization (SaaS, subscriptions).
9	Barriers to the implementation of digital auditing	Chambers (2025); Jupić & Gadžo (2023)	Identifies key obstacles to the digitalization of auditing: a skills gap, data security concerns, and organizational resistance.	Does not explore mechanisms for overcoming these barriers through the integration of audit into the product development processes of IT companies.
10	Specifics of IT service accounting and classification	Chernetska & Karnaukh (2023)	Examines business process architecture and classifies IT companies (product-based, service-based), justifying high operational risk.	Focuses on management accounting or service classification, bypassing digital internal audit tools for these processes.

As can be seen from Table 1, there is a structural gap in all ten research areas. In addition to significant progress in audit, maturity, and digitalization in Ukraine, it is necessary to note that there is no single conceptual framework that would be able to solve three important issues at once. First, the framework should take into account risks of sector accounting in connection with IT companies, such as IAS 38 related to capitalization of intangible assets and IFRS 15 concerning multi-element revenue recognition. Second, it should consider financial controls in the software development process. Third, the framework should be completely aligned with the European triad – CSRD, EU AI Act, and IIA Global Standards.

AIMS AND OBJECTIVES

In general, the main purpose of this research is to develop an evolutionary audit framework for IT companies that are currently undergoing digitalization and Europeanization. The specific goals are:

- analyzing sector-related risks in terms of accounting applicable to IT companies, especially in terms of intangibles and complications of revenue recognition models;
- creating an architecture that provides for the inclusion of financial controls into digital development processes (DevOps, CI/CD) according to the "Compliance as Code" concept;
- harmonizing the developed internal audit framework with the regulations of Central Europe, namely CSRD, EU AI Act, and the updated IIA Global Standards.

METHODS

The study relies on historical-logical, comparative, and systems analyses. A historical-logical approach traces the evolution of internal audit paradigms. We map the shift from retrospective documentary control to AI-driven preventive oversight across six decades of literature. Comparative analysis then evaluates existing maturity frameworks from KPMG, Clearsulting, and IIA Global Standards. This step positions the proposed five-stage model against current industry benchmarks. Finally, a systems approach integrates regulatory requirements, technological infrastructure (DevOps, CI/CD, ERP), and organizational roles into a cohesive architectural model.

Methodologically, this theoretical paper synthesizes peer-reviewed literature, normative frameworks, and existing maturity models. We construct an analytical framework to serve as a precursor for future empirical testing. The five-stage model acts as an analytical construct for theoretical generalization rather than a statistically derived taxonomy. The quantitative benchmarks cited here (ROI > 1.5, TTD < 24 hours, automation level > 75%) rely on professional literature instead of direct empirical validation. We propose them as normative targets, not established thresholds for the Ukrainian IT market. Primary limitations include a strict focus on SaaS and hybrid business models, with empirical validation currently limited to a dual-company case study, paving the way for broader statistical testing in future research.

Model Construction and Evaluation Framework

To construct the five-stage maturity model, this study employed a deductive synthesis method. The architectural foundation was derived from globally recognized IT governance and process maturity frameworks, specifically CMMI (Capability Maturity Model Integration) and COBIT 2019, combined with the updated Global Internal Audit Standards (IIA, 2024). These generalized frameworks were structurally recalibrated to address the unique accounting risks of the IT sector, namely, agile software development cycles, complex SaaS revenue recognition (IFRS 15), and the capitalization of intangible assets (IAS 38).

The selection of evaluation criteria for each stage (Audit Type, Toolkit, Automation Level, and Role in Decision-Making) was based on the fundamental paradigm shift from retrospective documentary control to preventive algorithmic governance. The Key Performance Indicators (KPIs), such as Time to Detect (TTD), Time to Remediation (TTR), and ROI, were determined through a synthesis of industry benchmarks (e.g., Deloitte, ISACA) and adapted for continuous auditing environments.

Algorithm for Transitioning Between Maturity Levels

The progression through the maturity model is not strictly linear but is governed by specific technological and organizational gateways (triggers):

1. Gateway to Stage 2 (Proactive): Requires the formalization of a risk matrix prioritizing IT-specific accounting risks and the initiation of targeted audits for high-risk areas (e.g., Diia.City compliance).
2. Gateway to Stage 3 (Analytical): The critical trigger is the deployment of an ERP system with open API capabilities and the integration of Business Intelligence (BI) platforms. This technological shift enables the transition from statistical sampling to 100% transaction coverage (Continuous Auditing).
3. Gateway to Stage 4 (Strategic): Triggered by the company scaling to multiple international markets and the subsequent necessity to integrate non-financial (ESG) reporting controls to comply with the Corporate Sustainability Reporting Directive (CSRD).
4. Gateway to Stage 5 (Predictive): Mandates the implementation of a mature DataOps infrastructure. The absolute prerequisite for this stage is the embedding of financial controls directly into CI/CD pipelines ("Compliance as Code"), supported by machine learning models capable of autonomous ex-ante blocking of erroneous transactions.

Integrated Maturity Level Assessment

Recognizing that corporate digitalization is often asynchronous, where cybersecurity controls might be highly advanced while IFRS 15 reconciliation remains manual, the model employs a multi-dimensional matrix algorithm for evaluation. The integrated maturity level of the internal audit function is not determined by the lowest common denominator. Instead, it is calculated as a weighted average of the maturity of individual audit processes (as demonstrated in the Results section). Process weights are assigned based on their material impact on financial statement accuracy and regulatory compliance risks, allowing IT companies to identify specific «bottlenecks» in their governance architecture.

DOI: 10.55643/fcaptp.4.69.2026.5290

In order to make the transition from the analytic stage to the predictive one economically feasible in digital auditing, it is necessary to develop the method of calculating return on investment (ROI). Based on the developed approach, the return on investment can be calculated by means of the formula:

$$ROI = \frac{B_{err} + S_{man} - C_{tec}}{C_{tec}}, \quad (1)$$

which takes into account the ratio of the net benefit from automation to the total cost of the technological infrastructure. The numerator consolidates the net effect: the sum of the benefits from error prevention (B_{err}) and direct savings on manual procedures (S_{man}), minus the cost of technological infrastructure (C_{tec}). The denominator, accordingly, consists of the cost of technological infrastructure (C_{tec}).

The assessment of the benefits of error prevention should be based on monetizing avoided regulatory fines and preventing losses resulting from the incorrect allocation of transaction prices under IFRS 15. Savings on manual procedures free up auditors for higher-level tasks, such as ESG and non-financial reporting. The denominator includes costs for cloud licenses, BI platforms, and ML development.

RESULTS

The specifics of accounting risks in IT companies as a catalyst for audit transformation

The modern-day scenario of the IT industry reflects a clear breakaway from the traditional concepts of industries. The assessment of worth in IT companies depends to a great extent on intellectual property, which shifts the focus of internal auditing from tangible inventory to virtual data flow. Operations in IT do not involve material expenses in any considerable quantity, but rely instead on a highly technological base, fast software updates, and complex, risky transactions. Managing such volatile environments necessitates a specialized methodology for analyzing the financial risks of IT sphere projects (Ostapets et al., 2026). Furthermore, the agility of the development process renders traditional documentation redundant.

The cost capitalization of software development can be viewed as the first significant area of risk. Furthermore, in the context of digital transformation, accurately disclosing the intangible value of a business, including goodwill, becomes a critical challenge for auditors. Intangible assets should be evaluated correctly by auditors, and for this purpose, there is a need to differentiate between the research phase and the development phase. However, given that in the case of iterative development methods and shortened release periods, these phases are very interrelated and create great uncertainty about their boundary, the lack of proper documentation makes it impossible to apply traditional control procedures. As a result, a shift towards an analytical approach is needed, in which special audit analytic modules analyze accounting information continuously concerning the engineers' billable hours using semantic algorithms for all technical activities. In this way, one can reveal instances where expenses related to bug fixing or technical maintenance are capitalized as costs associated with the development of some additional features, which is one of the most popular ways to inflate EBITDA.

The second significant area of risk is revenue recognition and peculiarities of accounting for IT services (Chernetska & Karnaukh, 2023). The introduction of IFRS 15 has changed the approach to accounting for SaaS companies completely. The specifics of contract formation in the sphere of IT services, especially when dealing with non-residents, define which model of revenue recognition is appropriate. Complex contracts including license fees, implementation, and support demand an elaborate identification of performance obligations and pricing. The IT industry is the leader in terms of risk of revenue manipulation caused by inappropriate revenue deferral (Napier & Stadler, 2020; EFRAG, 2024). Hence, internal audit of IT firms should move towards auditing the algorithms used by automated accounting systems for billing (KPMG International, 2024).

The third risk area, specific to the domestic IT market economy, entails the accounting of settlements with gig specialists and other personnel categories under the "Diia.City" regime: hybrid employment contracts, royalties, and author remunerations mandate a specialized audit procedure to reconcile accruals with the Ministry of Digital Transformation's resident registry. Misclassification of employment relations or violation of residency criteria invites substantial penalties and the retrospective accrual of tax liabilities under the general taxation system. For companies undergoing due diligence prior to securing venture capital, the accuracy of these settlements is a non-negotiable prerequisite, elevating the audit procedure of querying the Ministry's registry to compliance with European integration regulations.

The aforementioned specificities of accounting risks highlight the limitations of conventional digital audit methods, which are examined in the subsequent subsection.

ISSN: 2306-4994 | eISSN: 2310-8770 | Том 4 (69), 2026

Limitations of traditional methods and digital audit architecture

Transaction speed and intricacies of usage-based billing models make manual sampling controls ineffective. Sampled controls will not suffice for the detection of systemic ERP errors. Further development of export operations limits monitoring efforts outside of the digital space. The risk of financial statement misstatement exists as an integral part of the IT architecture in information technology businesses. Modern enterprises leverage DevOps along with CI/CD. Upon deployment of the script by a developer with errors in logic connected to subscription billing, the system automatically creates thousands of false entries in the ERP log. Thus, Continuous Control Monitoring becomes necessary for the validation of financial statements' accuracy. It is a systemic risk, not an intentionally committed fraud, which affects thousands of transactions at once without any physical paper trail.

Transformation of accounting processes is facilitated by digital transformation through the development of integrated platforms. Integration scripts connecting the CRM system, billing, and ERP systems implement the rules concerning price allocations and cost allocations. API gateways are the risk areas here, not static documents. Governance in such complex ecosystems requires the existence of an internal audit process to create an "Audit Layer," which will be a specially designed non-invasive layer. Such a layer will reconcile contracts, invoices, and revenue schedules on the side of the CRM, billing, and ERP systems, respectively. The "Compliance as Code" approach involves codifying the requirements for regulations, including IFRS and tax laws, into control rules, which are then embedded in the CI/CD pipeline as shown in Figure 1.

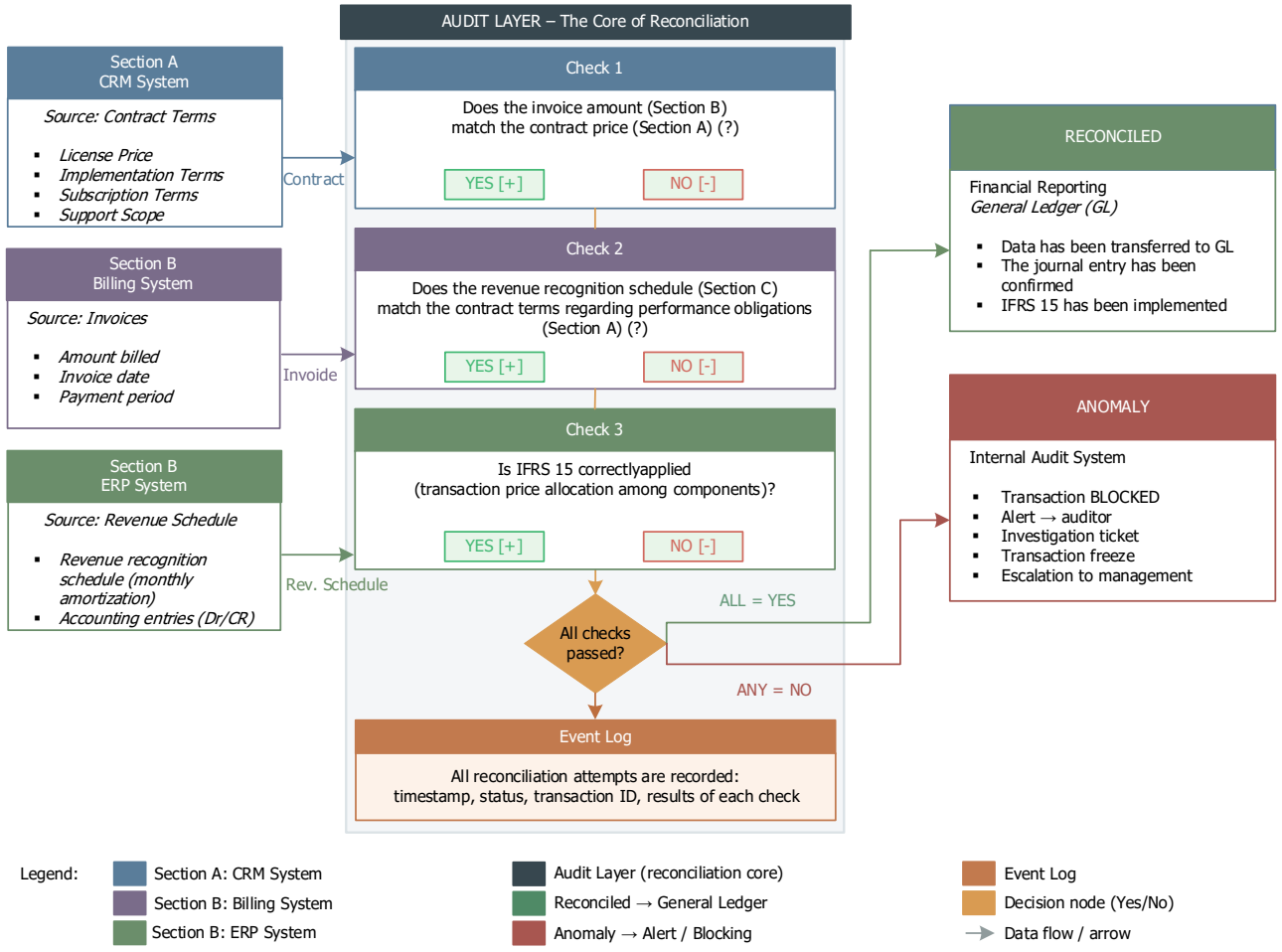

Figure 1. Architecture of data flows and internal audit control points in an integrated IT enterprise accounting system under the "Compliance as Code" paradigm.

Furthermore, within the "Compliance as Code" architecture, the system utilizes scripts to automatically tag Jira tasks using NLP and metadata. Such demarcation helps distinguish between the research stage and the subsequent capitalization of assets. In case a user attempts to finalize a bug fix ticket as a capitalized asset, an instant alert is raised as part of a preventive measure. Implementation of the blocking control mechanism in front of the gateways of the application programming interface of the accounting system provides a significant architectural benefit. The CI/CD pipeline pauses deployments in case any updated code violates transaction price allocation and expense classifications. This way, the system

DOI: 10.55643/fcaptp.4.69.2026.5290

prevents violations before any incorrect financial transactions can be booked into the ERP system. This model incorporates auditing as one of the essential elements of the development cycle, which helps ensure real-time compliance. At the most predictive level, the technical control is tightly integrated with an intelligent behavior profile. Such anomalies as unusual user behavior and possible collusion can be detected using artificial intelligence.

Transitioning to such an architecture is impossible without a profound evolution of the audit function itself, which we conceptualize as a five-stage maturity model (presented in Table 2). Within this framework, the Audit Layer architecture becomes viable at the Analytical Stage (Stage 3), where 100% of transactions are monitored. At the Predictive Stage (Stage 5), it transforms into an active "Compliance as Code" mechanism within CI/CD pipelines. The systemic trajectory of this transformation across all five maturity stages is detailed in the following subsection.

Detailing the stages of the evolutionary internal audit model

To systematically conceptualize the transformation of control functions, an original five-stage evolutionary model of accounting internal audit in IT companies was developed. This model synthesizes the frameworks of global internal audit institutes (The Institute of Internal Auditors, 2024) and the principles of data analytics-enabled auditing (Clearsulting, 2024; Firat, 2025).

Table 2. Evolutionary model of internal audit of accounting in IT companies (5 stages). Note: In Stage 3, controls are passive in nature (detecting errors after transactions have been executed), whereas in Stage 5, they become active (preventing errors during code deployment through "Compliance as Code" mechanisms)

Criterion	Stage 1: Reactive	Stage 2: Proactive	Stage 3: Analytical	Stage 4: Strategic	Stage 5: Predictive (AI-driven)
Audit type	Documentary audit after the close of the reporting period	Risk-based audit of key processes	Data-driven passive monitoring of 100% of transactions (post-factum)	Integration into the company's product lifecycle	Preventive audit "Compliance as Code"; active integration into CI/CD pipelines (ex-ante)
Main objective	Identification of errors in transaction recording, minimization of regulatory risks	Systematic risk assessment in key accounting processes	Comprehensive transaction analysis, identification of complex errors and anomalies in post-control mode.	Assessment of the accounting implications of new business models prior to launch	Autonomous prevention of errors and conflicts by blocking incorrect changes before they are deployed.
Audit targets	Accounting transactions at the aggregated level	Revenue recognition, intangible assets, digital assets, and subscriptions	100% of transactions, revenue recognition rules, and intangible asset amortization	Product lifecycle, monetization schemes, accounting policies	Product pre-concepts, pricing algorithms, smart contract code
Toolkit	Documentation procedures, spot checks	Basic analytical procedures, selective tests	SQL, BI platforms, continuous auditing/monitoring	Integration with design systems, assessment of impact on reporting	Machine Learning (anomaly detection), Digital Twins, Monte Carlo simulations
Level of automation	Limited access to IT infrastructure	Interaction with finance and IT departments during the change phase	Systematic use of analytics for passive monitoring of all stages of accounting	Full integration with ERP/CRM/billing systems	Standalone monitoring with active preventive blocking in CI/CD pipelines.
Role in decision-making	Retrospective control function, reporting adjustments	Participation in the business model transformation phase	Monitoring function, timely detection of deviations for correction	Full-fledged business partner, strategic advisor	Methodologist and architect of algorithmic prevention of accounting errors
Behavioral Audit Layer	Not available	One-time access checks upon request	Automated monitoring of event logs and access rights anomalies	Integration of UBA analytics with identity and access management (IAM) systems	Autonomous real-time detection of anomalous behavior by privileged users and collusions

According to the developed model, the evolution of internal audit progresses through five sequential stages. To comprehensively understand this transformation, it is expedient to combine theoretical descriptions with practical scenario modeling. Consider the evolution of controls using the example of a B2B agreement featuring multiple performance obligations (SaaS license, implementation, support), where the central IFRS 15 challenge is the allocation of the transaction price.

Stage 1: Reactive. This stage reflects the base maturity level, during which the internal audit process acts as the "controller of the past" (KPMG International, 2024). The procedures are limited to documentary post-closing audits, the scope of the work is based on sampling, and the level of automation is low.

Stage 2: Proactive. An increase in the volume of business operations requires a transition to a risk-oriented strategy. The internal audit focuses on the analysis of high-risk processes, such as revenue recognition according to IFRS 15, and privileged user access management.

Stage 3: Analytical. This stage reflects the qualitative development of technology: the auditors transition from sample-based procedures to Continuous Auditing (Clearsulting, 2024; Firat, 2025). Using business intelligence platforms and SQL queries, the auditors analyze the entire population of transactions (100%). This allows the identification of discrepancies between the contract terms and the schedule of revenue recognition (Digital Transformation, 2025) and log analysis to detect any irregularities in access rights permissions.

Stage 4: Strategic. On this level, internal audit is integrated into the digital product lifecycle. The auditors analyze the reporting effect of the price changes before implementation. The mandate of internal audit includes non-financial criteria, such as environmental, social, and governance (ESG) parameters and cybersecurity (Hecimovic & Canestrari-Soh, 2025).

This development corresponds to the ESG assurance maturity model consisting of four stages (de Leeuw & de Draaijer, 2025). The highest stage involves integration of non-financial auditing into corporate governance. Considering CSRD (2024) and Ukraine's EU accession commitments, the transition to strategic maturity becomes a mandatory regulatory requirement rather than a competitive advantage for domestic IT companies wanting to enter the European digital market.

The broadening of the scope of the internal audit process with the inclusion of ESG procedures becomes relevant for compliance with CSRD guidelines. Domestic IT companies willing to gain access to the EU market use KPIs not only for internal development but also for proof of compliance during the external audit performed by accredited auditors of the EU. The diversity of CSRD preparedness in European markets increases the significance of the issue. Zanócz (2025) finds, in his comparative analysis of non-financial reporting in Central European countries, significant differences in their preparedness for CSRD. To build a robust audit framework, domestic IT companies can also draw upon global empirical analyses of sustainability reporting audit determinants to benchmark their practices against broader international standards. In particular, while some countries are well-prepared, others are seriously lagging. This means that Ukrainian IT companies entering the EU market face the competition window when they have to make compliance-related investments. Behavioral auditing is integrated into IAM and uses UBA for insider threat detection.

Stage 5: Predictive (AI-driven). The peak of maturity involves switching to AI-based algorithmic governance, when the main goal changes from detecting an anomaly to preventing anomalies, making them impossible. NLP algorithms assess contract texts in CRM systems and identify variable consideration and multi-element obligations (Wassie & Lakatos, 2024; Chambers, 2025).

At the same time, the use of AI systems in auditing practice in the European Union is regulated by the EU AI Act (2024), which requires explainability (XAI) for algorithmic decisions. The application of XAI techniques to audit procedures (Damen et al., 2025) is crucial for certification of regulatory compliance of IT firms in EU markets. Moreover, the integration of AI into corporate governance demands a paradigm shift from mere technical compliance to algorithmic accountability and ethical business leadership in a digitally globalized environment (Szeberényi, 2026).

However, the main innovation is the "Compliance as Code" approach that involves integrating automated controls into CI/CD development processes. The script that does not conform to price allocation rules is prevented from entering the ERP system ex-ante. Such an approach provides compliance with the regulatory requirements as well as creates a verifiable data set for managerial accounting and project cost control. Therefore, such a high level of technical controls has certain limitations. It does not work in the case of management override or collusion that exploits weaknesses of the automated system, thus requiring continued operation of the behavioral monitoring system (Chambers, 2025; IIA, 2024).

Compliance of AI systems with the requirements of the EU AI Act represents another challenge at the level of prediction. The ECIIA (2025) roadmap designates internal audit as the major validation function of "high-risk" AI systems, especially for automated financial reporting decisions. For EU IT firms, such an approach represents a new mandatory audit task.

Financial misrepresentations that have the greatest impact are neither the result of programming errors nor mistakes but rather the result of circumventing CI/CD procedures and the development of hidden backdoors (Protiviti & IIA, 2023; Wassie & Lakatos, 2024). The only way to guard against both systematic failures and malicious managerial behavior lies in combining technical "Compliance as Code" and behavioral monitoring (Kononenko, 2024; Digital Transformation, 2025). The first and foremost requirement for implementing the above model is the clear specification of criteria indicating the movement between the levels of maturity. The next stage is unlocked when annual revenue exceeds USD 1 million or international markets are accessed. Transitioning to the third stage happens through the implementation of an ERP system with an API and the formation of a data team. The fourth stage is reached when three or more markets are scaled, and

DOI: 10.55643/fcaptp.4.69.2026.5290

non-financial reporting requirements arise. The fifth stage requires the development of a mature DataOps platform and an Artificial Intelligence Center of Excellence.

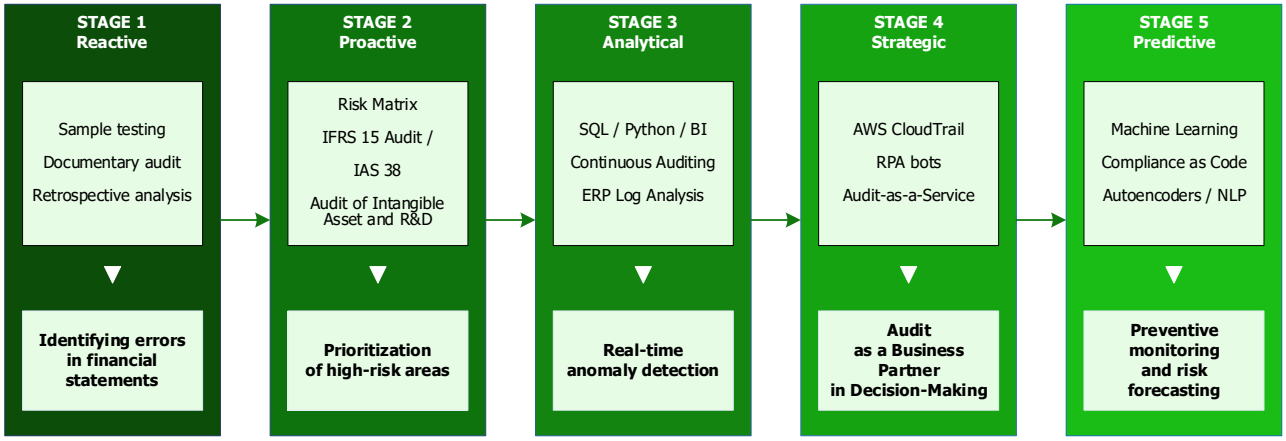

Figure 2. Five-stage model of internal audit evolution of accounting in IT companies.

According to recent research (Jupic & Gadzo, 2023; KPMG, 2024; Deloitte, 2025), the majority of companies in developing countries belong to the proactive stage (about 50-60%) of development, thus proving the presence of an "automation plateau", which means the necessity to adopt an evolutionary approach.

The five-stage model (Table 2, Figure 2) represents a necessary concept simplification that helps to demonstrate the general evolution pattern of the audit process. The transition from one stage to another is not always linear because many processes develop simultaneously. The conclusion is supported by the principles of the CMMI and COBIT frameworks (Myerson, 2016; Aguiar et al., 2018; Orbus Software, 2023; ISACA, 2011). Thus, the matrix approach could be used in practice, as exemplified in Table 3.

In this table, the rows represent various audit objects (revenue recognition, capitalization of intangible assets, "Diia.City" compliance, cybersecurity, ESG), while the columns correspond to the levels of development presented in Table 2. In this way, the matrix approach allows conducting a multidimensional self-assessment, which means the possibility of defining unique development paths of processes, as stated in modern research (Aguiar et al., 2018).

Table 3. Example of multi-dimensional maturity assessment of audit processes in an IT company. Note: The integrated maturity level is defined as a weighted average; the fact that it remains at Stage 3 despite the presence of individual Stage 5 processes illustrates the asynchronous nature of digitalization and the existence of "bottlenecks" in management.

Parameters and evaluation criteria	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Revenue Recognition (IFRS 15)					✓
Capitalization of Intangible Assets (IAS 38)			✓		
Compliance with "Diia.City"		✓			
Cybersecurity and access control		✓			
ESG reporting				✓	
INTEGRATED MATURITY LEVEL			✓		

The matrix approach expands on the baseline model by considering the varying levels of maturity among different audit processes, an issue that has significance especially for IT firms where technology and accounting maturity can be quite asynchronous. The implementation of "Compliance as Code" requires that a RACI matrix is developed for the seven key digital audit processes (Table 4).

Table 4. RACI Matrix for digital internal audit processes in IT companies. Note: R – Responsible (executor); A – Accountable (responsible for the result); C – Consulted (involved as an expert); I – Informed (informed).

Process / Tasks	Internal Audit	Finance Depart-ment	IT / DevOps	Senior Manage-ment
Development of a continuous audit architecture	A	C	R	I
Configuration of revenue recognition algorithms (IFRS 15)	C	A	R	I
Monitoring anomalies in transactions (AI/ML models)	A	C	R	I
Integrating tests into CI/CD pipelines	C	I	R	A
Audit of the capitalization of R&D and intangible asset costs (IAS 38)	A	R	C	I
Preparation of the audit report and recommendations	A	C	I	I
Monitoring compliance with the requirements of the "Diia.City" regime and IFRS 15	A	R	C	I

Transitioning to strategic and predictive stages demands abandoning traditional audit performance metrics. A customized system of KPI metrics is proposed to quantitatively gauge audit function efficacy across three dimensions: operational efficiency, risk management, and strategic value Table 5.

Table 5. System of KPI metrics for evaluating digital internal audit efficiency.

Assessment area	KPI metric name	Benchmark
Operational efficiency	Level of control automation	> 75% for mature IT companies (Stage 3+)
	Time to Detect (TTD)	< 24 hours; ideal – Real-time
Risk management	Audit coverage of data sets	100% (no sampling method)
	AI false positive rate	< 5%
	Percentage of detected anomalies confirmed as actual violations	> 80% (quality of ML models)
Strategic value	ROI of digital audit	> 1.5 (normative threshold derived from professional literature; see Discussion for derivation)
	TTR – Time to Remediation (time to resolve the detected violation)	< 72 hours
	Coverage of ESG processes by audit	> 30% for Stage 4 companies

To verify the adequacy of applying the ROI formula (1) defined in the methodology, let us consider a hypothetical mid-sized Ukrainian IT company (SaaS model, annual recurring revenue of USD 5 million) transitioning from Stage 2 to Stage 3. Assume annual benefits from prevented IFRS 15 misstatement penalties (B_{err}) of USD 120,000, savings on manual audit procedures (S_{man}) of USD 80,000, and total technology infrastructure costs (C_{tex}) of USD 100,000 per annum. Applying formula (1):

$$ROI = \frac{120000+80000-100000}{100000} = 1.0. \quad (2)$$

Since the ROI 1.0 result is under the ROI 1.5 mark, it shows that the predictive phase (Phase 5) is too early for an initial company and makes a transition through Phase 3 financially feasible. The more income and transactions there are, the more gains are generated compared to stable infrastructure costs. This usually results in increasing ROI above the feasible level of 1.7 to 2.3 (Deloitte, 2025).

Empirical validation and case study

To transition the proposed five-stage maturity model from a conceptual framework to a practically validated methodology, an empirical case study was conducted involving two mid-sized Ukrainian IT companies. Due to strict Non-Disclosure Agreements (NDAs) concerning internal financial controls, proprietary billing algorithms, and corporate security policies under martial law, the specific names of the entities are anonymized as Company A and Company B. Absolute financial figures are scaled or presented as relative ratios to ensure confidentiality, without compromising the scientific validity of the performance metrics.

DOI: 10.55643/fcaptp.4.69.2026.5290

To capture the sectoral nuances of the Ukrainian IT market, the selected companies represent two dominant, yet contrasting, business models operating under extreme conditions of distributed teams, cloud migration due to physical infrastructure risks, and strict compliance requirements of the "Diia.City" legal regime.

Case 1: Product-Based SaaS Company ("Company A")

Company A operates a B2B SaaS model aimed primarily at the EU and US markets. Due to martial law, its workforce is highly distributed, and all ERP and billing infrastructures were forcefully migrated to cloud environments (AWS/NetSuite) to ensure business continuity. The primary accounting challenge was the complexity of revenue recognition under IFRS 15, exacerbated by flexible subscription pauses and dynamic pricing models introduced to retain clients during geopolitical instability.

Prior to the digital transformation, the internal audit function operated at Stage 2 (Proactive), relying on retrospective sampling. The company initiated a transition towards Stage 5 (Predictive) by implementing the "Audit Layer" architecture. Financial controls were embedded directly into the CI/CD pipeline. Algorithms were deployed to autonomously verify transaction price allocations for multi-element arrangements before deployment. Any script updates that contradicted IFRS 15 revenue deferral policies were proactively blocked, eliminating the risk of systemic ERP contamination.

Case 2: Outsourcing/Service-Based Company ("Company B")

Company B is a mid-sized IT outsourcing provider navigating the mass transition of its workforce from the traditional Ukrainian Sole Proprietor (FOP) model to the new "Diia.City" gig-worker framework. The primary audit risks involved the misclassification of labor relations, the accurate capitalization of billable hours under IAS 38 across distributed project teams, and maintaining precise compliance with the Ministry of Digital Transformation's residency criteria. Losing resident status would revert the company to a standard, significantly higher corporate tax rate – a critical financial risk during an economic downturn.

Recognizing the budget constraints and the economic limitations of implementing a fully predictive AI-driven model for a Time & Material business, management targeted Stage 3 (Analytical). The transformation involved deploying Continuous Auditing tools (SQL scripts and Power BI) to passively monitor 100% of transactions. Automated daily reconciliation was established between the Jira time-tracking systems, gig-contractor payment registries, and the Diia.City compliance database.

Comparative Analysis of Efficiency Metrics

The implementation of the digital audit models yielded significant operational resilience for both companies over a 12-month observation period. The dynamic changes in key performance indicators (KPIs) are summarized in Table 6.

Table 6. Dynamics of KPI metrics in Ukrainian IT companies before and after the implementation of digital audit models.

KPI Metric	Company A (SaaS) Before (Stage 2)	Company A (SaaS) After (Stage 5)	Company B (Outsourcing) Before (Stage 1)	Company B (Outsourcing) After (Stage 3)
Audit coverage of data sets	< 5% (Targeted Sampling)	100% (Continuous)	< 10% (Targeted Sampling)	100% (Continuous)
Level of control automation	15%	88%	5%	72%
Time to Detect (TTD)	18–25 days (Post-close)	< 1 hour (Real-time)	30+ days	< 24 hours
Diia.City compliance monitoring	Manual / Quarterly	Continuous AI monitoring	Manual / Bi-annually	Automated daily alerts
Unrecognized IFRS 15 anomalies	High risk	0 (Algorithmic prevention)	Moderate risk	Near 0 (Daily alerts)
ROI of digital audit	N/A	2.4	N/A	1.7

Discussion of Empirical Findings

The empirical findings confirm the theoretical criteria proposed in the methodology by applying them in the high-risk operational environment. The transition of Company A to Predictive maturity led to an ROI of 2.4. In the SaaS approach, the correction of the systematic IFRS 15 misstatements quickly compensated for the considerable infrastructure investments. The capability of blocking errors on its own played a critical role during the times when human audits were unable to be performed due to some external threats (e.g., power failure or relocation).

At the same time, for Company B, the achievement of Stage 3 provided a strong ROI of 1.7. Based on the empirical findings, it is necessary to point out that for the outsourcing approaches, when the main problem is regulatory compliance (loss of Diia.City, for example) rather than errors in fast transactions, passive continuous monitoring is the most economically justified stage of maturity.

Thus, the study proves that the best maturity stage varies according to the company's business model and regulations.

DISCUSSION

As demonstrated by the ROI modeling in the previous section, the transition to advanced audit stages requires careful economic justification. Unlike the markets in North America or Western Europe where legacy systems are preventing digitalization, there is a peculiar anomaly about the IT infrastructure in Ukraine: while having up-to-date cloud systems, local businesses experience structural segregation between the development teams and the control functions. Thus, the technological infrastructure is not the primary obstacle to maturity; instead, cultural factors and the CFO's leadership come into play here. As a consequence, the viability of investments in digital audit goes beyond ROI alone and also depends on the willingness of management to implement changes within the organization.

The proposed "Compliance as Code" system represents the change in the control vector of Continuous Auditing (Firat, 2025; Wassie & Lakatos, 2024), moving from post-fact detection to pre-emptive control of code deployment. The proposed solution directly tackles the problem raised in Napier and Stadler (2020), according to which the problems with IFRS 15 reporting result not from misstatement but from algorithm errors.

The established ROI threshold of ≥ 1.5 can be considered a practical contribution to the debate about the thesis of Jupić and Gadžo (2025), since it takes into account the cost of capital (WACC) and the risks of AI tools becoming obsolete, as well as possible fines under the CSRD and the EU AI Act. Those aspects significantly affect the breakeven point for transformation for firms targeting the European market. In response to arguments about universal automation, it should be noted that from the perspective of investment analysis, investments in machine-learning architecture are unprofitable for companies with low revenues. When the predicted ROI level is below the proposed threshold, starting the predictive phase is not appropriate and may reduce the value of the firm. For companies at Stages 3-4 of maturity, the average ROI is 1.7-2.3 (median of 1.8-2.0) (Deloitte, 2025). Thus, the evolutionary nature of the digital shift is evident. Achievement of the above-mentioned level becomes a reasonable basis for making budget requests before presenting them to the audit committee.

Limitations of the study

A particularly significant limitation of the application of the model relates to taking into account the time horizon of the expected results. As it follows from empirical studies carried out by Eulerich et al. (2025), the positive results of continuous auditing become evident only two to three years after its introduction. Thus, the above-mentioned result highlights the importance of using a strategic approach to the realization of Stage 3.

In addition, it is crucial to state that the main obstacles that prevent the process of audit digitalization relate to the lack of qualified auditors who are competent in financial control and use digital technologies, the lack of legislation regulating AI compliance in Ukraine, and limited budgets of audit departments. Martial law implies that the transformation takes place within strictly determined phases (KPMG, 2025; Jupić & Gadžo, 2023).

Based on cross-sector statistics (Deloitte, 2025), it is shown that digitization of the audit function becomes financially sustainable at an ROI of 1.5 or more. The mentioned ROI takes into account the costs related to compliance risk under the CSRD and EU AI Act. Furthermore, while according to the literature the maturity level of predictive auditing (Stage 5) is characterized by the full (100%) audit of transactional databases and the time-to-detect (TTD) of less than 24 hours, these metrics operate as normative standards of implementation but not as empirical results obtained in the course of current research. It stresses the scientific importance of the research, which distinguishes theoretical benchmarks from real-life implementation in emerging economies.

CONCLUSIONS

As a result of the performed study, a systematic analysis of the transformation of internal audit systems in IT companies was carried out, leading to the following key conclusions in line with the main goals of the research project:

DOI: 10.55643/fcaptp.4.69.2026.5290

First, in connection with the evaluation of sectoral risks in accounting, it was proven that the main flaws of sampling audit techniques make them unusable in the context of advanced SaaS business models and fast automated transactions typical of the IT sector. Taking into account the fact that any distortions of finances in this environment appear as a result of systemic failures of billing algorithms, not random mistakes of an individual, reliable financial reporting requires proactive blocking of algorithmic errors at the implementation stage, combined with AI behavioral monitoring.

Secondly, to solve this problem, an evolutionary maturity model of IT internal audits was created, which implies a transition from retrospective detection to preventive measures. At its core is a concept of "Compliance as Code" where financial controls (for example, IFRS 15) are embedded into the DevOps/CI/CD technology stack. In addition, a set of practical tools, including a RACI matrix and a set of specially designed KPIs, was developed.

Thirdly, from a theoretical perspective, this research contributes to placing mature audit frameworks into the concrete technological context of IT enterprises. From a practical point of view, the model is useful for helping IT companies developing in the framework of the European single market to proactively prevent systemic financial risks, fill in the gap between IT and finance departments, and build natural alignment of internal controls with the standards of CSRD and EU AI Act.

Prospects for further research. The results can serve as a basis for future empirical validation of the multidimensional maturity assessment and normative parameters (such as ROI and TTD) for a larger sample of Ukrainian IT companies. In addition, taking into account the European integration path, creating special audit protocols to test compliance and "explainability" of AI tools within the framework of the EU AI Act becomes crucial for future research.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Aguiar, J., Pereira, R., Vasconcelos, J. B., & Bianchi, I. (2018). An overlapless incident management maturity model for multi-framework assessment (ITIL, COBIT, CMMI-SVC). *Interdisciplinary Journal of Information, Knowledge, and Management, 13*, 137–163. https://doi.org/10.28945/4083
2. Baharom, Z. (2025). Theoretical and practical insights into digital technologies in internal auditing: A bibliometric analysis of trends and future directions (1980–2024). *Discover Data, 3*, Article 41. https://doi.org/10.1007/s44248-025-00081-z
3. Chambers, R. (2025, December 9). *Five barriers slowing AI adoption in internal audit*. Audit Beacon. https://www.richardchambers.com/five-barriers-slowing-ai-adoption-in-internal-audit/
4. Chernetska, O. V., & Karnaukh, S. D. (2023). Oblikove zabezpechennia protsesu nadannia IT-posluh na pidpryiemstvi. *Biznes Inform, 10*, 259–264. https://doi.org/10.32983/2222-4459-2023-10-259-264
5. Clearsulting. (2024). *5 levels of internal audit automation maturity*. https://www.clearsulting.com/insights/blog/5-levels-internal-audit-maturity/
6. Damen, V., Wiersma, M., Aydin, G., & van Haasteren, R. (2025). Explainable AI for EU AI Act compliance audits. *Maandblad voor Accountancy en Bedrijfseconomie, 99*(4), 231–242. https://doi.org/10.5117/mab.99.150303
7. De Leeuw, R., & de Draaijer, A. (2025). Internal audit's strategic role in sustainability and ESG transformation. *Maandblad voor Accountancy en Bedrijfseconomie, 99*(4), 243–250. https://mab-online.nl/article/167721/
8. Deloitte. (2025). *AI and tech investment ROI*. Deloitte Insights. https://www.deloitte.com/us/en/insights/topics/digital-transformation/ai-tech-investment-roi.html
9. DOU.ua. (2025). *Minus 20 tysiach fakhivtsiv v Ukraini: Yak povnomasshtabna viina vplynula na top-50 IT-kompanii.* https://dou.ua/lenta/articles/top-50-three-years-of-war/
10. European Confederation of Institutes of Internal Auditing. (2024). *Risk in focus 2025: Hot topics for internal auditors*.

https://www.eciia.eu/wp-content/uploads/2024/09/Risk-in-Focus-2025-FINAL.pdf

11. European Confederation of Institutes of Internal Auditing. (2025). *The AI Act: Road to compliance*. https://www.eciia.eu/wp-content/uploads/2025/01/The-AI-Act-Road-to-Compliance-Final.pdf

12. European Financial Reporting Advisory Group. (2024). *Post-implementation review of IFRS 15 – Issues paper*. EFRAG Financial Reporting Technical Expert Group and Consultative Forum of Standard Setters meeting. https://www.efrag.org/system/files/sites/webpublishing/Meeting%20Documents/2312131548185581/08-01%20PIR%20IFRS%2015%20-%20Issues%20paper%20-%20EFRAG%20FR%20TEG-CFSS%202024-03-13.pdf

13. Eulerich, M., Bamberg, A., Bonrath, A., Kordes, J., & Wagener, M. (2025). How Deutsche Telekom uses emerging technologies to enhance the internal control system. *Journal of Emerging Technologies in Accounting, 22*(2), 79–96. https://doi.org/10.2308/JETA-2023-054

14. Eulerich, M., Fligge, B., López Kasper, V. I., & Wood, D. A. (2025). Patience is key: The time it takes to see benefits from continuous auditing. *Accounting Horizons, 39*(1), 69–86. https://doi.org/10.2308/HORIZONS-2023-060

15. Fırat, Z. (2025). Yapay zekânın muhasebe denetiminde kullanımı: Fırsatlar, zorluklar ve gelecek yönelimleri. *Muhasebe Bilim Dünyası Dergisi, 27*(2), 77–95. https://doi.org/10.31460/mbdd.1577715

16. Hecimovic, A., & Canestrari-Soh, D. (2025). Strategies for internal auditors to expand their role in ESG assurance. *The British Accounting Review*. Advance online publication. https://doi.org/10.1016/j.bar.2025.101805

17. IFRS Foundation. (2014). *IFRS 15: Revenue from contracts with customers*. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/

18. IFRS Foundation. (2024). *Academic literature review: Post-implementation review of IFRS 15*. https://www.ifrs.org/content/dam/ifrs/resources-for/academics/research-citations/pir-ifrs-15-literature-review-may-2024.pdf

19. Instytut vnutrishnikh audytoriv Ukrainy. (2024). *Hlobalni standarty vnutrishnoho audytu.* https://www.iia.org.ua

20. ISACA. (2011). *COBIT mapping: Mapping of CMMI for development V1.2 with COBIT 4.1*. https://www.isaca.org

21. Jupić, N., & Gadžo, A. (2025). Enhancing small and medium enterprise performance through artificial intelligence integration in accounting. In *SMEPP 2025: Zbornik radova* (pp. 33–46). Univerzitet u Novom Pazaru. https://www.econstor.eu/bitstream/10419/324135/1/CLANAK-SMEPP-ENG.pdf

22. Kononenko, L. V. (2024). Vykorystannia suchasnykh tsyfrovykh tekhnolohii v audyti: Problemy ta perspektyvy. *Ekonomichnyi Prostir, 192*, 109–112. https://economic-prostir.com.ua/wp-content/uploads/2024/09/192-109-112-kononenko.pdf

23. KPMG. (2025). *The new Global Internal Audit Standards*. https://kpmg.com/be/en/insights/risk/new-global-internal-audit-standards.html

24. KPMG International. (2024). *Implementing IFRS 15: Revenue from contracts with customers*. https://assets.kpmg.com/content/dam/kpmg-sites/xx/pdf/ifrg/2024/isg-kpmg-comment-letter-pir-of-ifrs15-revenue-from-contracts-with-customers.pdf

25. Lviv IT Cluster. (2026). *IT research Ukraine 2025*. https://itcluster.lviv.ua

26. Ministerstvo finansiv Ukrainy. (1999). *Natsionalne polozhennia (standart) bukhhalterskoho obliku 15 "Dokhid" (Nakaz No. 290 vid 29.11.1999).* Zakonodavstvo Ukrainy. https://zakon.rada.gov.ua/laws/show/z0860-99#Text

27. Myerson, J. (2016). *How CMMI models compare and map to the COBIT framework*. TechTarget. https://www.techtarget.com/searchsecurity/tip/How-CMMI-models-compare-and-map-to-the-COBIT-framework

28. Napier, C. J., & Stadler, C. (2020). The real effects of a new accounting standard: The case of IFRS 15 revenue from contracts with customers. *Accounting and Business Research, 50*(5), 474–503. https://doi.org/10.1080/00014788.2020.1770933

29. Opendatabot. (2026). *Diia.City: Pidsumky 2025 roku.* https://opendatabot.ua/analytics/diia-city-2025

30. Orbus Software. (2023). *A look at the Innovation Value Institute*. Orbus Software Blog. https://www.orbussoftware.com/resources/blog/post/a-look-at-the-innovation-value-institute

31. Ostapets, A., Parasii-Verhunenko, I., Bezverkhyi, K., Matiukha, M., & Yurchenko, O. (2026). The development of analysis methodology of financial risks of projects in IT sphere. *Technology Audit and Production Reserves, 1*(4(87)), 6–20. https://doi.org/10.15587/2706-5448.2026.352430

32. Papinko, A. I. (2024). *Upravlinskyi oblik biznes-protsesiv v IT-kompaniiakh* [Doctoral dissertation, Zakhidnoukrainskyi natsionalnyi universytet]. https://dspace.wunu.edu.ua/bitstream/316497/50101/1/Dis%20Papinko%20%D0%90.pdf

33. Protiviti & The Institute of Internal Auditors. (2023). *11th annual global technology audit risks survey*. https://www.protiviti.com/sites/default/files/2023-10/11th-annual-global-technology-audit-risks-survey-iia-protiviti-2023.pdf

34. PwC. (2024). *Implementing the IIA's Global Internal Audit Standards*. https://www.pwc.com/gx/en/services/audit-assurance/internal-audit/new-global-internal-audit-standards.html

35. SafePaaS. (2025). *Continuous monitoring in IT audit*. https://www.safepaas.com/articles/continuous-monitoring-in-it-audit/

36. Shukurova, N. M., & Plevako, N. O. (2020). Suchasnyi stan ta tendentsii rozvytku ukrainskykh pidpryiemstv IT-haluzi v umovakh tsyfrovykh transformatsii. *Ekonomika: Realii Chasu, 4*, 71–77. https://doi.org/10.15276/ETR.04.2020.10

DOI: 10.55643/fcaptp.4.69.2026.5290

37. Szeberényi, A. (2026). From compliance to accountability in digital globalization: The ethical friction threshold model for artificial intelligence-enabled business leadership. *Business Ethics and Leadership, 10*(2), 228–243. https://doi.org/10.61093/bel.10(2).228-243.2026

38. The Institute of Internal Auditors. (2024). *Global internal audit standards*. https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/

39. Tsyfrova transformatsiia bukhhalterskoho obliku ta audytu v Ukraini. (2025). *Visnyk Lvivskoho natsionalnoho universytetu pryrodokorystuvannia. Seriia: Ekonomika, 16*(3–4), 45–54. https://visnyk.lnau.edu.ua/index.php/economics/article/view/435

40. Wassie, F. A., & Lakatos, L. P. (2024). Artificial intelligence and the future of the internal audit function. *Humanities and Social Sciences Communications, 11*(1), 1–13. https://doi.org/10.1057/s41599-024-02905-w

41. Zanócz, A. (2025). Non-financial reporting and assurance trends in selected Central European countries. *Public Finance Quarterly, 71*(3), 94–115. https://doi.org/10.35551/PFQ_2025_3_4

Басін А., Петрик О., Матієнко-Зубенко І., Кузик Н., Мельник Л.

ЕВОЛЮЦІЯ ВНУТРІШНЬОГО АУДИТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ IT-КОМПАНІЙ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Об’єктом дослідження є система внутрішнього аудиту IT-компаній в умовах цифрової трансформації та європейської інтеграції. Головною проблемою аудиту IT-компаній є критична неефективність традиційних і ретроспективних підходів у випадку швидких автоматизованих операцій, складних багатокомпонентних механізмів визнання доходів і хмарних ERP-систем.

Метою дослідження є узагальнення існуючих моделей зрілості та узгодження процесів внутрішнього аудиту з вимогами європейських нормативних актів, а саме: Директиви про корпоративну звітність щодо сталого розвитку (CSRD), Закону ЄС про штучний інтелект (EU AI Act) і МСФЗ 15. Також ураховане внутрішнє регулювання правового режиму «Дія Сіті» в Україні. З методологічного погляду в дослідженні застосовані історико-логічний, порівняльний і систематичний аналізи для оцінки існуючих парадигм і створення структурної аналітичної рамки.

Основними результатами дослідження є п’ятиступенева еволюційна модель зрілості внутрішнього аудиту, яка розвивається від реактивної базової парадигми до прогностичної парадигми з використанням штучного інтелекту. Моделювання етапів призвело до створення архітектури «Audit Layer» і «Compliance as Code». Вимоги фінансового контролю реалізовано у вигляді автоматизованих перевірок у конвеєрах DevOps і CI/CD відповідно до запропонованої архітектури. У результаті парадигма аудиту перейшла від виявлення помилок ex-post до прогнозування помилок ex-ante з автономним блокуванням некоректних фінансових операцій, зокрема неправильного розподілу ціни операції. Також для оцінки ефективності аудиту розроблено матрицю RACI та скориговану систему KPI.

Основні висновки показують, що поєднання алгоритмічного блокування та моніторингу поведінки з використанням штучного інтелекту (ШІ) усуває розрив між IT- та фінансовими підрозділами компанії. Це має важливе значення для масштабування діяльності IT-компаній на європейському цифровому ринку. Крім того, економічна доцільність переходу до просунутих аналітичних етапів доведена розрахунком рентабельності інвестицій (ROI) ≥ 1,5, що враховує фінансові ризики, пов’язані з недотриманням нормативних вимог.

Ключові слова: внутрішній аудит, IT-компанії, цифрова трансформація, Compliance as Code, безперервний аудит, модель зрілості, ефективність аудиту, операційна ефективність, автоматизований контроль, європейська інтеграція

JEL Класифікація: M41, M42, F15, L86