The Eurasia Proceedings of
Educational and Social Sciences (EPESS)
ISSN: 2587-1730

The Eurasia Proceedings of Educational and Social Sciences (EPESS), 2026

Volume 48, Pages 60-72

IConMEB 2026: International Conference on Management Economics and Business

Auditing AI-Based Systems in Banking Information Security: Auditors' Perceptions and Expectations

Judit Schubert
Obuda University

Agnes Csiszarik-Kocsir
Obuda University

Abstract: The application of artificial intelligence (AI) in banking information systems poses new types of security, control and oversight challenges. The research aims to explore how IT auditors perceive and evaluate the tasks, risks and expectations related to auditing AI-based systems. The study uses a qualitative methodology to collect data from the professional community, with a particular focus on issues of transparency, verifiability, explainability and information security. The research presents the main risks identified by auditors – such as opacity of models, uncertainties in data quality, lack of reproducibility of decision processes and potential biases – as well as the opportunities that arise from the application of AI, such as increased efficiency, automated controls or improved anomaly detection. It also identifies the factors that determine the auditability of AI systems in the field of banking information security, including the quality of documentation, the regulation of model development processes, monitoring mechanisms and organizational maturity. The results contribute to the professional discourse on the methodological and practical frameworks of AI auditing and may inform the development of future regulatory, supervisory and audit practices. The study also highlights that the role and competencies of auditors are also changing with the spread of AI-based systems, creating new knowledge and skill needs in the profession.

Keywords: AI-audit, Information security, IT audit, AI act, Agile, Lean

Introduction

The rapid expansion of artificial intelligence (AI) is fundamentally transforming the operation of information security in the banking sector, creating new types of risks, control tasks, and supervisory expectations. In the financial industry, AI-based systems—particularly machine learning models, predictive analytics, and automated decision-support solutions—are playing an increasingly significant role in fraud prevention, risk management, and customer behavior analysis. At the same time, the need to ensure transparency, explainability, and auditability is growing, as these are essential prerequisites for information security and effective assurance processes.

AI auditing, however, cannot yet be considered a routine practice: the professional community worldwide is still searching for the methodological, technological, and regulatory frameworks that would enable the evaluation of complex, often "black-box" models. The regulatory environment – particularly the AI Act and the GDPR – places increasing emphasis on the transparency and risk management of AI systems, indicating that AI auditing is likely to become an integral part of banking information security in the near future.

The aim of the research is to explore how IT auditors in the Hungarian banking sector perceive the tasks, risks, and expectations associated with auditing AI-based systems. The study places particular emphasis on issues of transparency, explainability, data quality, methodological frameworks, and organizational maturity. By applying an integrated mix of qualitative and quantitative methods, the research analyzes the perceptions of a focus group of auditors and identifies the key factors that determine the auditability of AI systems in the banking environment.

This research represents the first stage of a longer-term longitudinal study. A follow-up assessment is planned in three years, enabling the comparison of auditors' perceptions, competencies, and the evolution of the regulatory environment over time. Accordingly, the present study not only maps the current state of AI auditing in the banking sector but also establishes a baseline for evaluating future trends and directions of development.

Theoretical Background

Relevance of Agile and Lean Operating Models in Auditing

Agile and Lean operating models have become increasingly influential in banking and IT environments over the past decade, and they are exerting a growing impact on audit activities as well. The rapidly evolving technological landscape, the emergence of AI-based systems, and the need for continuous development cycles have made it necessary for the audit function to adapt to more flexible, iterative ways of working. The following section examines how Agile and Lean approaches contribute to audit effectiveness and why they are particularly relevant in the assessment of AI systems (Hyperproof, 2025).

Agile methodology originally emerged in software development, but it has since been widely adopted across various business domains. Its core elements – iterative processes, continuous feedback, collaboration, and rapid responsiveness – align well with the challenges of the modern audit environment. According to the literature, the purpose of agile auditing is to enable the audit function to respond to organizational changes in a more flexible, timely, and risk-sensitive manner (Deloitte, 2024; Wolters Kluwer, 2021). Agile auditing:

- operates in shorter cycles (sprint-based auditing),
- maintains continuous communication with stakeholders,
- relies on the ongoing reassessment of risks,
- enables rapid correction and shifts in focus.

Traditional annual audit planning often struggles to keep pace with the rapidly changing technological environment, particularly in the case of AI systems, where models and data evolve continuously. Agile auditing is therefore especially relevant in the assessment of AI-based systems, as their operation is iterative, dynamic, and frequently only minimally documented.

Lean Perspective and Its Applicability to Auditing

Lean management aims to simplify processes, reduce waste, and maximize value creation. The purpose of Lean auditing is to:

- reduce unnecessary administrative activities,
- shorten audit cycles,
- increase the value-creating nature of audits,
- focus on the most critical risks.

The Lean approach is particularly important in the banking environment, where processes are complex, documentation requirements are extensive, and the auditing of AI systems demands significant resources. Lean auditing helps ensure that auditors do not become overwhelmed by excessive detail but instead focus on the areas posing the greatest risk – such as model transparency, data quality, and governance processes. According to the literature, Lean auditing increases audit efficiency and reduces cycle time while improving stakeholder satisfaction (Paterson, 2015; Rathod, 2024).

The Relationship Between Agile and Lean Auditing and the Assessment of AI Systems

Auditing AI-based systems is an area where traditional audit approaches are often insufficient. Model behaviour is dynamic, data inputs change continuously, and development cycles are iterative. As a result, the auditing of AI systems naturally aligns with Agile and Lean principles. Agile and Lean auditing are particularly relevant for the following reasons:

- Iterative model development: AI models are often built through sprint-based development cycles, which requires the audit process to be iterative as well.
- Continuous risk assessment: The risk profile of models may change over time, making continuous monitoring essential for effective auditing.
- Addressing transparency gaps: Agile auditing facilitates close collaboration with development teams, which is crucial for reducing the "black-box" nature of AI systems.
- Efficiency gains: Lean auditing helps focus on the most critical AI-related risks while eliminating unnecessary control steps.

It is important to emphasize that, for example in credit-rating processes, machine-learning models can only be applied responsibly if banks are able to ensure their transparency, auditability, and explainability, as the "black-box" nature of such models poses significant risks for consumers, auditors, and supervisory authorities (Bücker et al., 2020).

Regulatory Environment: AI Act, GDPR, and Banking Compliance in the Auditing of AI Systems

Although the banking sector is already one of the most heavily regulated industries in Hungary, the use of artificial intelligence in banking information security is taking place within a regulatory environment that is rapidly evolving and aims to ensure transparency, safety, and accountability in the case of high-risk technologies (Barta, 2021). From the perspective of AI auditing, three regulatory pillars are particularly influential: the EU AI Act, the GDPR, and the supervisory expectations applicable to the banking and financial sector (EBA, ECB, MNB). Together, these frameworks shape the environment in which auditors must evaluate the operation, risks, and compliance of AI-based systems.

The Role of the EU AI Act in Ensuring Auditability

The AI Act is the first comprehensive, risk-based AI regulation that assigns high-risk AI systems to a dedicated category—this includes banking applications such as credit-scoring, fraud-prevention, and risk-management models. The regulation requires, among other things:

- ensuring model transparency,
- mandating documentation and logging obligations,
- maintaining a quality-management system,
- operating effective risk-management processes,
- providing mechanisms for monitoring and post-market oversight.

These requirements are directly linked to auditability: understanding model behaviour, ensuring reproducibility, and maintaining high-quality documentation are all areas that the focus-group participants also identified as critical. According to the literature, the AI Act is expected to significantly increase both the number and the depth of AI audits, as demonstrating compliance will only be possible through structured audit processes (Floridi et al., 2023; European Commission, 2024). In addition to prescribing several criteria governing the operation of AI systems, the regulation cannot yet be considered fully comprehensive. The provisions of the Act will require further refinement and regular review in the future (Antal & Számadó, 2025).

GDPR and Data Governance: A Cornerstone of AI Auditing

Although the GDPR is not an AI-specific regulation, it plays a fundamental role in the auditing of AI systems, as the functioning of machine-learning models depends heavily on the quality, origin, and management of the data they rely on. The GDPR is particularly relevant in the following areas:

- data quality and accuracy,
- purpose limitation in data processing,
- accountability,
- data-subject rights,
- transparency in automated decision-making.

International literature highlights that achieving GDPR compatibility is one of the most challenging aspects of AI auditing, as the training data of machine-learning models is often heterogeneous, insufficiently documented, or

difficult to trace (Wachter et al., 2023; Kaminski, 2022). This aligns with the perceptions of your focus group: according to participants, the lack of data quality and data governance represents one of the most critical obstacles.

Banking Compliance and Supervisory Expectations

In the banking sector, the auditing of AI systems is shaped not only by EU-level regulation but also by the expectations of financial supervisory authorities. The EBA, the ECB, and the MNB all emphasize:

- the importance of model-risk management,
- the necessity of model validation,
- the strengthening of documentation and control environments,
- the transparency of governance processes.

According to the EBA's 2021 guidelines, explainability, continuous monitoring, and bias assessment are particularly critical for machine-learning models, as these constitute fundamental prerequisites for auditability. The focus-group responses indicate that Hungarian auditors perceive these areas as the most critical as well.

The Relationship Between Regulation and Auditability

The regulatory environment therefore simultaneously represents:

- a compass (as it defines expectations),
- a framework (as it sets the conditions for compliance),
- a barrier (as practical implementation is not yet fully mature).

According to the focus-group participants, current regulation "provides direction but does not provide tools." This duality also appears in the international literature: the methodological and technological foundations of AI auditing are still emerging, and regulatory developments often evolve more rapidly than the level of organisational preparedness (Brundage et al., 2022; Tiganila, 2024).

International Trends in AI Auditing

AI auditing is a rapidly evolving field worldwide, shaped simultaneously by technological innovation, regulatory expectations, and organisational risk-management practices. International literature and leading institutions (NIST, OECD, ENISA, ISACA, IIA) consistently indicate that the auditability of AI systems will become strategically significant in the coming years, particularly in high-risk sectors such as banking and financial services.

The Global Rise of Transparency and Explainability as Strategic Priorities

According to international research, the greatest obstacle to AI auditing is the opacity and "black-box" nature of many models. The lack of transparency is not only a technological issue but also a legal and ethical one, as it directly affects accountability and compliance.

- The three-layer audit framework proposed by Floridi and colleagues (governance, technical assessment, impact evaluation) has become one of the most influential models in the international discourse, built on strengthening transparency and reproducibility (Mökander et al., 2023).
- The NIST AI Risk Management Framework (2023) likewise emphasises that explainability and high-quality documentation are essential prerequisites for auditability.

The trend is clear: transparency is not optional but the starting point of AI audits.

Yu and Kumbier (2017) argue that the reliability of AI systems can only be ensured if human–machine collaboration is embedded throughout development and evaluation, grounded in the core principles of statistical thinking — population, question, representativeness, and critical scrutiny (PQRS).

The Strengthening of AI Risk-Management and Governance Frameworks

International organisations are developing increasingly detailed guidelines for managing the risks of AI systems, and these frameworks directly influence audit practice.

- According to ISACA's 2023 report, most organisations still lack AI-specific control environments, even though risk-management expectations are rising rapidly (ISACA, 2023).
- OECD and ENISA emphasise a lifecycle-based perspective in which auditing is not a one-off activity but requires continuous monitoring and post-deployment oversight.

The governance-centred approach is therefore strengthening globally, and audit practices must adapt accordingly.

Regulatory Compliance as a Driver of AI Auditing: The AI Act and the GDPR

One of the most significant drivers of international trends in AI auditing is regulation. The EU AI Act is the world's first comprehensive AI regulation, which makes the following elements mandatory for high-risk systems:

- detailed documentation,
- risk-management processes,
- a quality-management system,
- monitoring and post-deployment oversight.

The GDPR remains equally influential, particularly due to its requirements on data quality, accountability, and the transparency of automated decision-making (Kaminski, 2022). The international trend is therefore moving increasingly toward regulation-driven auditing.

Technological Enablement of AI Auditing: Tools and Automation

In international practice, an increasing number of organisations are deploying AI to support the auditing of AI systems themselves, including:

- model-monitoring tools,
- bias-detection algorithms,
- automated documentation-analysis systems.

According to Brundage et al. (2022), the future of AI auditing lies in the "verifiable claims" approach, in which developers make evidence-based, testable assertions about model behaviour, and auditors verify these claims. This trend is particularly relevant in the banking sector, where model-risk management is already heavily regulated (Oláh, 2025).

Competency Gaps and the Global AI Skills Shortage

International research consistently indicates that one of the greatest obstacles to AI auditing is the shortage of qualified professionals and the widening skills gap. According to the World Economic Forum, the demand for AI-related competencies is growing faster than the supply of trained specialists. Surveys by ISACA and the IIA likewise show that most auditors do not feel adequately prepared to conduct AI audits. The international literature also highlights that AI auditing still lacks a unified, widely accepted methodology. Current trends point toward:

- the hybridisation of existing frameworks (NIST + ISACA + OECD),
- lifecycle-based auditing,
- risk-based approaches,
- the integration of technical and non-technical controls.

Scholars agree that methodological consolidation is expected in the coming years, accelerated by the compliance requirements introduced by the AI Act.

Materials and Methods

The study was based on semi-structured interviews conducted with eleven IT auditors. The interview protocol included both open-ended questions and closed Likert-scale items. Using the same set of questions for all participants ensured comparability across responses. This design enabled the integrated analysis of both quantitative and qualitative data.

Results

The aim of the research was to explore how IT auditors and internal controllers working in the banking sector perceive the tasks, risks, and expectations associated with auditing artificial intelligence–based systems. The study employed both qualitative and quantitative methods: in addition to the Likert-scale and open-ended items included in the questionnaire, focus-group interviews were also conducted. Building on the survey results, this chapter presents respondents' perceptions, the emerging patterns, and the key conclusions. Most participants in the sample were IT auditors working in a banking environment, typically with either 0–3 years or 8–15 years of professional experience. A smaller proportion of respondents were internal auditors. Approximately one-third of the participants had already been involved in auditing AI-based systems, which allows for the comparison of differences based on prior experience.

Demographic Characteristics of the Respondents

The respondents' demographic characteristics show that 80% of participants work in IT-audit roles, while the remaining share are internal auditors. In terms of organisational background, nearly all respondents came from banking institutions, which aligns well with the focus of the study.

The distribution of professional experience reveals three distinct groups:

- 0–3 years of experience: nearly half of the respondents
- 8–15 years of experience: a substantial proportion
- 15+ years of experience: a smaller but professionally influential group

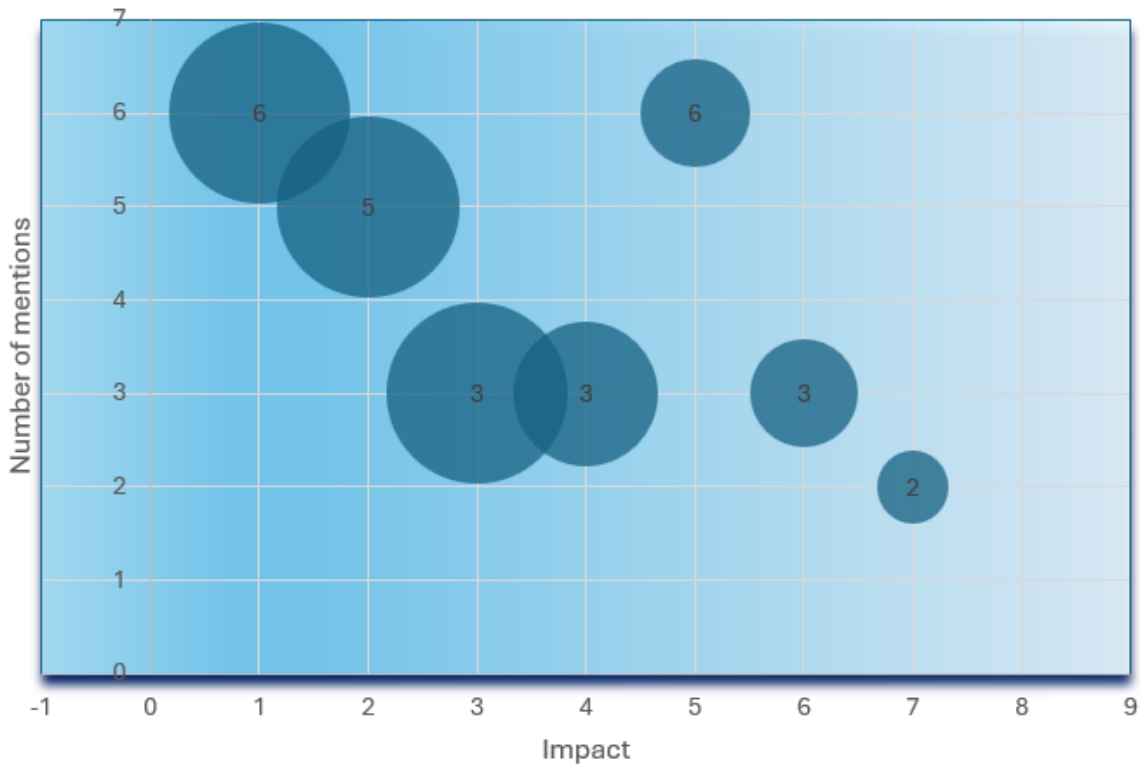

Figure 1. Source: Author's own research, 2026, n = 11

For analytical purposes, respondents were categorised into two experience levels: those with 0–3 years in audit were classified as juniors, while those with at least eight years of experience were considered seniors. This distinction is reflected in the polarisation observed in several response patterns. Approximately 30% of respondents had previously participated in AI-related audits, typically involving machine-learning models or fraud-detection systems.

Most participants indicated that the competencies required for AI auditing are only partially available within their current skill set. Their self-assessment generally fell within the "somewhat agree" to "mostly agree" range, suggesting that auditors recognise existing knowledge gaps but do not consider themselves entirely unprepared. Perceptions of organisational support were mixed: several respondents noted that their organisation had provided certain training opportunities, though these were often not AI-specific or lacked sufficient depth.

The bubble chart in Figure 1 visualises the frequency of mentions for the following themes: understanding AI functionality, model transparency, data quality and data governance, lack of technological knowledge, methodological gaps, access and collaboration challenges, and limited practical experience. Categories rated as having an impact level of 5, 6, or 7 were considered critical by all respondents, indicating that without these elements AI auditing is practically infeasible. Categories rated 4 or 3 were viewed as important but not prohibitive, while category 2 reflected issues that are more experiential than structural (see Table 1).

Table 1. Categories and justifications

Category	Impact (1–5)	Justification
Understanding the Functioning of AI Systems	5	This is the most critical competency: if the auditor does not understand how the model operates, they cannot meaningfully assess the associated risks.
Model Transparency and Reproducibility	5	The "black box" phenomenon represents the greatest obstacle to the auditability of AI systems. This was also the most frequently mentioned concern among the respondents.
Lack of Methodological and Audit Frameworks	5	The current audit frameworks were not designed for AI, which makes this a systemic barrier.
Data Quality and Data Governance	4	It is a critical factor, though the responses suggest it is less dominant than transparency or methodological adequacy.
Lack of Technological Knowledge	3	It is important, yet partly compensable through training; its impact does not manifest equally across all auditors.
Issues of Access and Collaboration	3	It is a significant barrier, yet one that can be addressed at the organisational level; it does not constitute a fundamental technological or methodological issue.
Lack of Practical Experience	2	It is primarily characteristic of junior auditors; it is important, yet it does not constitute a systemic barrier.

Comparison by Level of Experience

The interview responses reveal a clear distinction between the perspectives of senior and junior auditors. Notably, both groups perceive the methodological frameworks as insufficient. Neither junior nor senior auditors consider the current audit frameworks suitable for assessing AI systems, and professional experience does not appear to reduce methodological uncertainty. The issues of transparency and reproducibility are likewise dominant across both groups. Senior auditors report that they cannot "infer" how the model operates, and they emphasise that the black-box phenomenon constitutes a barrier regardless of experience level.

In the category of lacking technological knowledge, responses were provided primarily by participants with 0–3 years of experience. Their answers suggest that junior auditors have had fewer encounters with AI systems. Senior auditors, by contrast, tended to highlight methodological and governance-related challenges. In the category concerning lack of practical experience, two responses came from junior auditors. Based on the data, junior auditors more frequently mention the lack of technological knowledge and practical experience. Senior auditors, on the other hand, place greater emphasis on the absence of methodological frameworks, transparency issues, and governance-level obstacles. Access and collaboration challenges appear in both groups. This indicates that organisational barriers are not experience-dependent, and that cooperation with model-development teams constitutes a systemic issue.

The comparison by experience level shows that there is no substantial difference between senior and junior auditors in how they perceive the methodological and transparency-related challenges of AI audits. Both groups consider methodological gaps and model opacity to be highly critical, suggesting that these challenges cannot be compensated for by professional experience.

Among junior auditors, references to lacking technological knowledge and practical experience are more common, whereas senior auditors focus more on methodological and governance-level issues. Access and collaboration difficulties are present in both groups, pointing to organisation-level barriers. Overall, experience does not reduce the complexity of AI audits: senior and junior auditors alike perceive the lack of methodological frameworks and the transparency challenges of AI models as significant obstacles.

Pareto Analysis of the Three Main Categories

To summarise the results of the qualitative coding, I applied a Pareto analysis to examine the extent to which the problems mentioned by respondents concentrate around a few dominant categories. The three most frequent categories are:

Table 2. Dominant categories

Category	Number of mentions
Understanding the Functioning of AI Systems	6
Methodological Gaps	6
Model Transparency	5

Total mentions: 6 + 6 + 5 = 17
Total Number of Mentions: 6 + 6 + 5 + 3 + 3 + 3 + 2 = 28
Pareto- Ratio: $\frac{17}{28} \approx 61\%$

Sixty-one percent of all problems mentioned by respondents concentrate in just three categories. Although this does not reach the classical 80% threshold, it still represents a strong Pareto effect, clearly highlighting the focal points of perceived challenges. Based on the Pareto analysis, the majority of issues identified by respondents cluster around three key areas: understanding how AI models function, the lack of methodological frameworks, and model transparency. This indicates that the most significant barriers to AI auditing are not scattered, minor issues but rather a set of systemic and interrelated challenges. The fact that 61% of all mentions fall into these three categories demonstrates that perceptions within the professional community are highly concentrated: the fundamental prerequisites for AI auditability are perceived as lacking, regardless of experience level.

Thematic Analysis of Open-Ended Responses

Based on the qualitative data, four main areas of competence gaps emerge:

- Understanding the functioning of AI systems (“understanding the AI-based operation of specific applications”)
- Interpreting the internal logic of models (“understanding the internal logic of AI applications”)
- Knowledge of data quality and data governance (“knowledge of data quality and data governance”)
- Updating technological knowledge (“keeping up-to-date with the latest technologies”)

The responses indicate that the lack of preparedness stems primarily from deficits in technological and methodological knowledge rather than from shortcomings in core auditing skills.

The four competence areas identified through the qualitative responses clearly demonstrate that the difficulties encountered in AI auditing do not arise from weaknesses in traditional auditing competencies. Instead, they reflect the fact that AI-based systems introduce technological and methodological challenges that extend beyond the boundaries of conventional audit frameworks. Respondents consistently emphasised that understanding how AI systems operate and interpreting the internal logic of models represent the most substantial obstacles. The “black-box” nature of AI, the complexity of algorithms, and model-specific operational characteristics form a domain in which the current auditor knowledge base is insufficient.

Closely related to this is the lack of knowledge regarding data quality and data governance, as the performance and reliability of AI models fundamentally depend on the quality and management of the underlying data. The need to continuously update technological knowledge further highlights that the rapidly evolving AI landscape requires ongoing learning—something for which current organisational and training structures are not yet adequately prepared.

Overall, the responses suggest that the lack of preparedness does not stem from weaknesses in auditing skills but from the fact that evaluating AI systems requires new, specialised technological and methodological expertise. These competence gaps are therefore systemic: AI auditing is an area where traditional audit frameworks offer limited guidance, and where professional development hinges on strengthening technological and data-driven capabilities.

Opportunities Arising from the Use of AI According to the Interview Findings

Although most respondents primarily emphasised methodological, technological, and transparency-related challenges, the interviews also revealed several areas where AI-based systems offer substantial opportunities for the audit function. These opportunities align with international trends, yet—based on the perceptions of Hungarian banking auditors—they can also be interpreted as concrete, practical benefits.

Efficiency Gains and Shorter Audit Cycles

Several respondents highlighted that the use of AI-based systems in the audit process can significantly reduce the time required for audit procedures. According to the responses, AI:

- is capable of rapidly processing large volumes of data,
- supports the replacement of manual checks,
- enables continuous rather than merely periodic monitoring.

This is particularly important in the banking environment, where both the volume and complexity of transactions are high.

Automated Controls and Continuous Monitoring

Several interviewees noted that AI-based systems can enable the creation of automated controls that:

- are capable of signalling irregularities in real time,
- reduce risks arising from human error.
- support the continuous operation of the control environment.

One respondent explicitly emphasised that “meaningful progress would require having direct professional experience in the field,” suggesting that the introduction of AI-enabled controls can generate substantial value when accompanied by deeper domain expertise.

Advanced Anomaly Detection and Enhanced Risk Identification

Respondents highlighted that one of the greatest advantages of AI lies in its ability to recognise patterns and detect anomalies at an early stage. Based on practical experience, AI can identify relationships and irregularities that traditional tools are unable to capture, supports predictive risk management, and enhances the effectiveness of fraud detection systems. This is particularly relevant in the context of banking information security, where threats evolve rapidly.

Strengthening the Professional Role of the Auditor

Interview findings suggest that AI-based systems do not diminish the role of the auditor; rather, they shift it toward higher value-added activities. Instead of manual checks, the emphasis moves to model validation, the assessment

of data quality, and the evaluation of governance processes. Several respondents noted that AI auditing "requires complex knowledge and a broader perspective," which, in the long term, contributes to the professionalisation and strengthening of the audit function.

Future Outlook

Most respondents believe that AI-enabled audits will become routine in the future; however, this will require:

- substantial competence development,
- clearer and more detailed regulatory frameworks,
- the establishment of AI-specific audit methodologies. Based on the responses, the role and competencies of auditors are expected to undergo significant transformation.

Interpretive Summary

Based on the findings of the study, interest in AI auditing is high among the auditors participating in the focus group; however, gaps in preparedness, methodological foundations, and regulatory frameworks pose significant obstacles. The most critical factor is the lack of model transparency, which fundamentally affects auditability. Deficiencies in organisational maturity and collaboration further complicate the examination of AI systems. Respondents clearly expressed the need for standardised control frameworks, more detailed documentation, and AI-specific training. Overall, the study highlights that AI auditing requires system-level developments across multiple dimensions, including competencies, regulation, methodology, and organisational processes.

Perceptions Related to Regulation

Based on the questionnaire responses, it is clear that a significant proportion of participants perceive the auditability of AI-based systems primarily as a matter of regulatory uncertainty. Although the professional community is aware that the AI Act and the GDPR increasingly address transparency, risk management, and data-handling requirements for AI systems, the responses indicate that the current regulatory environment is not considered sufficiently concrete or practically applicable.

Among the methodological gaps, several respondents noted that regulation "provides direction but not tools." This suggests that auditors do not view regulation merely as a background condition but as a framework whose shortcomings directly affect auditability. According to the responses, the greatest difficulty lies in the fact that regulation articulates expectations – such as transparency, explainability, and data quality – without specifying how these should be assessed in practice.

Issues of transparency and reproducibility appear particularly prominently. Respondents pointed out that although regulation requires AI systems to operate transparently, this is often not realised in banking practice: development teams do not always provide adequate documentation, model behaviour is not reproducible for external parties, and explainability tools are not consistently available. As a result, a substantial gap exists between regulatory expectations and actual system behaviour.

In the areas of data quality and data governance, respondents also identified regulatory challenges. GDPR compliance – especially regarding the origin, quality, and handling of training data – remains an area where organisations lack mature practices. Several participants emphasised that the auditability of AI models depends heavily on the documentation of data-handling processes and the traceability of data-quality assurance.

Forward-looking responses reveal that most auditors view regulation as a key driver of change. They expect AI audits to become routine in the near future, with the implementation of the AI Act playing a central role. At the same time, the responses also show that the professional community does not yet feel fully prepared to ensure regulatory compliance: while the current frameworks are seen as directional, they are not considered detailed enough to provide a stable foundation for day-to-day audit practice.

Overall, the questionnaire results indicate that regulation functions both as a point of reference and a source of uncertainty. It provides direction by outlining the future trajectory of AI auditing and increasingly clarifying expectations. Yet it also introduces uncertainty, as the methodological and technological structures required for

practical implementation are not yet in place. Based on respondents' perceptions, regulation currently offers a framework rather than concrete guidance, and this duality significantly shapes how AI auditing is understood and practiced.

Interpreting Competence Gaps and Their Alignment with International Trends

Based on the qualitative responses, four closely interrelated competence areas emerge that shape the difficulties experienced in AI auditing: understanding how AI operates, grasping the internal logic of models, knowledge of data quality and data governance, and the need for continuous updating of technological expertise. These competence gaps clearly indicate that the lack of preparedness does not stem from weaknesses in core auditing skills, but rather from the fact that AI-based systems introduce technological and methodological challenges that extend beyond traditional assurance frameworks.Respondents' perceptions align closely with international trends. Global literature and leading organisations (NIST, OECD, ENISA, ISACA) consistently highlight that the greatest barrier to AI auditing is model opacity and the "black-box" nature of AI systems, which complicates understanding system behaviour and uncovering decision logic. The lack of transparency is widely recognised as one of the most critical issues worldwide, and it appears as the second most frequently mentioned challenge in the sample. Similarly, deficiencies in data quality and data governance are internationally regarded as key threats to the reliability of AI systems, mirroring respondents' expressed need for stronger data-driven practices and more robust governance frameworks.

The need for continuous technological upskilling is likewise a global phenomenon. Research by the World Economic Forum and ISACA shows that the pace of technological development outstrips the capacity of training systems, resulting in a persistent skill gap. The interview findings reflect this precisely: junior auditors report technological knowledge gaps, while senior auditors point to methodological and governance-level deficiencies—together forming the same competence deficit identified internationally in the context of AI auditing.

Overall, respondents' perceptions are well aligned with international trends: the competence gaps are systemic and stem primarily from the technological complexity of AI systems, the opacity of models, and shortcomings in data-governance structures. These challenges shape the global trajectory of AI auditing and reinforce the conclusion that strengthening professional preparedness requires continuous expansion of both technological and methodological expertise.

Conclusions

The findings of the study indicate that auditing AI-based systems in the banking sector introduces new types of challenges that extend beyond traditional assurance frameworks. According to respondents' perceptions, the most critical obstacles stem from gaps in technological and methodological knowledge rather than weaknesses in core auditing competencies. The four identified competence gaps – understanding how AI operates, grasping the internal logic of models, knowledge of data quality and data governance, and the need for continuous technological upskilling – clearly demonstrate that AI auditing requires new dimensions of professional preparedness.

The results of the Pareto analysis further reinforce this picture: more than half of the identified issues concentrate in just three key areas, suggesting that the major barriers to AI auditability are systemic and interdependent. The minimal differences between junior and senior auditors' perceptions indicate that experience alone is insufficient for evaluating AI systems; the nature of the challenges requires new forms of expertise that current training and methodological frameworks do not yet provide.

Comparison with international trends shows that domestic perceptions closely align with global patterns. Lack of transparency, the "black-box" nature of models, data-quality issues, and the skill gap resulting from rapid technological development are among the most critical obstacles to AI auditing worldwide. The findings therefore reflect not only the challenges of local practice but also fit within a broader international context.

Looking ahead, several directions emerge. First, there is a need for methodological frameworks specifically designed to support the auditability of AI systems and adaptable to agile and Lean operational models. Second, targeted competence development is essential: auditors require technological, data-driven, and model-level knowledge that enables deeper understanding and evaluation of AI systems. Third, strengthening organisational

collaboration – particularly among development, data-management, and security teams – is crucial for improving auditability.

Scientific Ethics Declaration

* The authors declare that the scientific ethical and legal responsibility of this article published in EPESS journal belongs to the authors.

Conflict of Interest

* The authors declare that they have no conflicts of interest.

Funding

* This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Management Economics and Business (www.iconmeb.net) held in Budapest/Hungary on February 05-08, 2026.

References

Antal,T., I., & Számadó, R. (2025). Út az elmélettől a gyakorlatig: A mesterséges intelligencia európai uniós szabályozásának elemzése – ajánlás az általános felhasználási feltételekre. *Biztonságtudományi Szemle, 7*(4), 167–188.

Barta, G. (2023). *A digitális transzformáció hatása a vállalati működésre* (Doctoral dissertation). Magyar Agrár- és Élettudományi Egyetem.

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., Khlaaf, H., Maharaj, T., Anderljung, M., Brown, R., Leike, J., & Clark, J. (2022). Toward trustworthy AI development: Mechanisms for supporting verifiable claims. *arXiv*. Retrieved from https://arxiv.org/abs/2004.07213

Bücker, M., Szepannek, G., Gosiewska, A., & Biecek, P. (2020). Transparency, auditability and explainability of machine learning models in credit scoring. *arXiv*. Retrieved from https://arxiv.org/pdf/2009.13384.pdf

Deloitte. (2024). *Putting agile change into action: It starts with teams. Deloitte Insights*. Retrieved from https://action.deloitte.com/insight/3831/putting-agile-change-into-action-it-starts-with-teams

Deloitte. (n.d.). *Agile internal audit: Planning, performance and value.* Retrieved from https://www.deloitte.com

Hyperproof. (2025). *Agile auditing: What to know*. Retrieved from https://hyperproof.io/resource/agile-auditing-what-to-know/

Kaminski, M. E. (2022). The right to contest AI. *Columbia Law Review, 122*(8), 1957–2040. Retrieved from https://columbialawreview.org/content/the-right-to-contest-ai/

Mökander, J., Schuett, J., Kirk, H. R., & Floridi, L. (2023). Auditing large language models: A three-layered approach. *Oxford Internet Institute*. Retrieved from https://arxiv.org/abs/2302.08500

Oláh, R. (2025). Mesterséges intelligencia a kiberbiztonságban: Anomáliák nyomában (gépi tanulási technikák alkalmazása hálózati anomáliák detektálására). *Biztonságtudományi Szemle, 7*(3), 167–175.

Paterson, J. C. (2015). *Lean auditing: Driving added value and efficiency in internal audit*. John Wiley & Sons.

Rathod, H. (2024). Building a better auditor: Embracing agile audit. *Internal Auditor Magazine*. Retrieved from https://internalauditor.theiia.org/en/voices/2024/october/building-a-better-auditor-embracing-agile-audit/

Tiganila, C. (2024). *Artificial intelligence audit and risk management toolkit*. ISACA. Retrieved from https://www.scribd.com/document/894128933/ISACA-Artificial-Intelligence-Audit-and-Risk-Management-Toolkit

Wolters Kluwer. (n.d.). *What is agile auditing?.* Retrieved from https://www.wolterskluwer.com/en/expert-insights/what-is-agile-auditing

Yu, B., & Kumbier, K. (2017). Artificial intelligence and statistics. *arXiv*. Retrieved from https://arxiv.org/abs/1712.03779

Author(s) Information

Judit Schubert
Óbuda University, Doctoral School on Safety and Security Sciences, J321, 3rd Floor, 6 József Boulevard, 1088 Budapest, Hungary
ORCID iD: https://orcid.org/0009-0007-7377-1163.
*Contact e-mail: *schubertj1983@gmail.com*

Ágnes Csiszárik-Kocsir
Óbuda University, Keleti Károly Faculty of Business and Management, Tavaszmező Street 15–17, H-1084 Budapest, Hungary
ORCID iD: https://orcid.org/0000-0001-5454-7843

*Corresponding authors contact email

To cite this article:

Schubert, J., & Csiszárik-Kocsir, Á. (2026). Auditing AI-based systems in banking information security: Auditors' perceptions and expectations. *The Eurasia Proceedings of Educational and Social Sciences (EPESS), 48,* 60-72.