TACJE

TRANSNATIONAL ACADEMIC JOURNAL OF ECONOMICS

*Transnational Academic Journal of Economics, Year: 2025, Volume: 2, Issue: 3, Pages : 241-250* *Research Article*

**DOI: 10.5281/zenodo.18442968**

Publication Date: 30.09.2025

Harun Tahiri[1]

1. University of Tetovo, Tetovo, North Macedonia Str. Ilinden, nn., 1200 Tetova, North Macedonia ORCID: 0009-0009-1771-2067
Email: harun.tahiri@unite.edu.mk

# Artificial Intelligence in Accounting and Auditing: Automation Bias, Internal Control Redesign, and EU AI Act Compliance in Regional Supply Chains

## Abstract

Artificial intelligence (AI) is rapidly transforming accounting and audit functions through automation, anomaly detection, and predictive analytics. Simultaneously, it introduces new assurance and governance risks, particularly "automation bias"—the propensity of users to over-trust algorithmic recommendations and reduce professional skepticism. This paper examines how automation bias affects audit judgment, internal control effectiveness, and compliance readiness under the European Union Artificial Intelligence Act (European Union, 2024). Using a socio-technical risk model and control-mapping approach aligned with COSO Internal Control–Integrated Framework and ISA 315 (Revised 2019) (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013; International Auditing and Assurance Standards Board [IAASB], 2019), the study proposes a practical governance blueprint for companies and audit firms operating in Western Balkan supply chains connected to EU markets. Findings emphasize that AI-enabled controls can increase coverage and timeliness, but may degrade control reliability without robust human oversight, explainability, monitoring, and model risk management. A compliance roadmap integrates AI Act obligations with audit evidence requirements and risk management standards (National Institute of Standards and Technology [NIST], 2023; International Organization for Standardization [ISO], 2023).

**Keywords:** AI in auditing; automation bias; internal control; EU AI Act; model risk management; supply chain compliance

How to cite: Tahiri H. Artificial Intelligence in Accounting and Auditing: Automation Bias, Internal Control Redesign, and EU AI Act Compliance in Regional Supply Chains. *Transnational Academic Journal of Economics, 2*(3), 241-250

## 1. Introduction

AI adoption in accounting and auditing is no longer experimental: it increasingly underpins transaction matching, exception identification, continuous controls monitoring, and audit planning. These applications promise efficiency gains, broader coverage than traditional sampling, and improved detection of anomalous patterns. Yet the same characteristics that make AI attractive—speed, complexity, and statistical authority—can amplify cognitive and organizational failure modes, notably automation bias: decision-makers may defer to model outputs, discount conflicting evidence, and reduce professional skepticism. This risk is particularly salient in auditing, where skepticism and judgment are foundational to risk assessment and evidence evaluation under international standards (IAASB, 2019).

Regulatory and market forces further elevate the stakes. The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) establishes a risk-based framework for AI systems placed on the EU market or used within the EU, including obligations for certain "high-risk" systems, transparency duties, governance requirements, and post-market monitoring (European Union, 2024; White & Case, 2024). Although many Western Balkan firms operate outside the EU, supply-chain integration, cross-border service provision, and EU client expectations increasingly require alignment with EU AI governance norms. In practice, this affects: (i) finance and accounting shared services supporting EU entities; (ii) external audit engagements of regional subsidiaries of EU groups; and (iii) supplier compliance programs required by EU customers.

This paper addresses a critical convergence problem: audit and assurance frameworks are evolving to incorporate advanced analytics and AI, while AI governance regulation (AI Act) imposes compliance constraints that can alter system design, documentation, and controls. A purely technical implementation of AI may improve operational performance but undermine assurance if it reduces traceability, creates opaque model risk, or shifts accountability away from humans. Similarly, a compliance-first approach can become a "paper program" if it fails to address real cognitive and control failures such as automation bias.

The study focuses on three research questions:

1. **RQ1:** How does automation bias manifest in accounting and auditing workflows, and what are its primary risk pathways?
2. **RQ2:** How should internal control systems be redesigned to manage AI-induced risks while preserving auditability and reliability (COSO, 2013; IAASB, 2019)?
3. **RQ3:** What practical compliance roadmap aligns AI-enabled accounting/audit tools with EU AI Act requirements in cross-border supply chains? (European Union, 2024; Orrick, 2024)

## 2. Materials and Methods

### 2.1 Research design and analytical approach

This paper uses a structured conceptual-methods design suitable for governance and assurance research where direct access to proprietary audit datasets is limited. The approach combines:

- **Regulatory analysis** of EU AI Act structure, phased applicability, and governance obligations (European Union, 2024; White & Case, 2024).
- **Assurance mapping** to international auditing standards, with emphasis on risk assessment and IT understanding under ISA 315 (Revised 2019) (IAASB, 2019).
- **Internal control mapping** to COSO Internal Control–Integrated Framework (2013), focusing on control environment, risk assessment, control activities, information & communication, and monitoring (COSO, 2013; AICPA & CIMA, 2013).
- **AI risk management synthesis** based on NIST AI RMF and ISO/IEC 42001 as practical governance scaffolding (NIST, 2023).
- **Literature synthesis** on automation bias, algorithmic bias, and AI ethics in auditing and decision-making (Musyoka, 2024; Romeo & Conti, 2025).

### 2.2 Operational definitions

- **Automation bias:** systematic over-reliance on algorithmic outputs, including omission errors (failing to act because the system did not flag an issue) and commission errors (accepting an incorrect recommendation) (Romeo & Conti, 2025).
- **AI-enabled control:** a control activity or monitoring process that depends on algorithmic inference (classification, anomaly detection, forecasting) rather than deterministic rules.
- **Auditability:** the ability to generate sufficient appropriate evidence, including traceability of inputs, model logic (or surrogate explanations), change logs, and performance monitoring.

### 2.3 Model: socio-technical risk pathways

The mechanism model (Figure 1) identifies five linked pathways:

1. data and feature risks; 2) model risks; 3) user cognition risks (automation bias); 4) organizational governance risks; and 5) compliance/assurance breakdown risks.

### 2.4 Supply chain compliance context

The paper treats “regional supply chains” as networks where non-EU firms provide goods/services to EU customers or operate as subsidiaries/vendors of EU-regulated entities. The compliance relevance is driven by extraterritorial commercial pressure and contractual governance rather than formal legal applicability in every case; nonetheless, firms placing AI systems on the EU market or using them in EU contexts face direct obligations (European Union, 2024; Cambridge University Press, 2024).

## 3. Results

### 3.0 Synthesis of findings

The analysis indicates that AI adoption increases coverage and speed but introduces material risks to control reliability and audit judgment. The most consequential risks arise when (i) decision workflows become "AI-first," (ii) humans are not trained to challenge outputs, and (iii) model governance lacks documentation, monitoring, and change control.

### 3.1 Automation bias as an assurance risk

Automation bias is particularly dangerous in audit and controllership settings because the professional expectation is not merely operational efficiency, but skeptical evaluation of evidence and risk. ISA 315 (Revised 2019) strengthens requirements around understanding the entity, IT environment, and risk assessment rigor—areas directly affected when AI systems shape transaction flows and monitoring (IAASB, 2019).

In accounting operations, automation bias manifests when staff accept AI-coded exceptions (e.g., "likely duplicate invoice," "low risk vendor") without independent verification, leading to omission errors. In external audit, it can manifest as over-trust in analytics that narrow substantive testing, even when underlying data quality or model drift is unverified. Automation bias risk increases when model outputs are presented with high confidence scores, when explainability is weak, and when organizational culture equates "technology" with "correctness."

The literature on AI in auditing highlights ethical and bias concerns, including transparency and accountability gaps (Musyoka, 2024). More recent reviews emphasize that automation bias is not eliminated by simply "keeping a human in the loop"; effective human oversight requires structured challenge protocols, training, and clear accountability for override decisions (Romeo & Conti, 2025).

**Control implication:** automation bias should be treated as a control risk and mapped into COSO's risk assessment and monitoring components (COSO, 2013).

### 3.1.1 Internal control redesign and EU AI Act alignment

The EU AI Act imposes governance expectations consistent with lifecycle controls: risk management, data governance, technical documentation, transparency, human oversight, accuracy/robustness/cybersecurity, and post-market monitoring—especially for high-risk systems and certain model categories (European Union, 2024; Orrick, 2024). Even when a specific accounting AI tool is not "high-risk" by legal classification, EU customers and auditors increasingly request comparable evidence: model documentation, control logs, and monitoring results.

Internal control redesign should therefore incorporate **model risk management (MRM)** as a formal control domain. Practically, this means:

- **Governance controls:** defined model owner, approval gates, segregation of duties between developers and validators.
- **Data controls:** lineage, completeness, bias testing, and access control for training/production datasets.
- **Operational controls:** threshold management, override protocols, and dual-review for high-impact outputs.
- **Monitoring controls:** drift detection, periodic performance back-testing, incident response.

NIST AI RMF provides a structured risk management lifecycle (govern, map, measure, manage) that can be integrated into COSO monitoring and risk assessment processes (NIST, 2023). ISO/IEC 42001 further supports an organizational management-system approach for AI governance, improving standardization and auditability of AI-related processes (ISO, 2023).

**Figure 1 (Mandatory)**

**Figure 1. Automation bias and AI governance risk pathways in accounting and auditing (socio-technical model)**

AI deployment in accounting/audit (classification, anomaly detection, forecasting)
→ **(1) Data risk:** incomplete/biased features; weak lineage
→ **(2) Model risk:** opacity; drift; calibration errors
→ **(3) Human risk:** automation bias; reduced skepticism; over-trust in confidence scores
→ **(4) Governance risk:** unclear accountability; weak change control; poor documentation
→ **(5) Assurance/compliance failure:** insufficient audit evidence; control breakdown; EU AI Act nonconformity exposure (European Union, 2024)

*(Cited in text as Figure 1.)*

**Table 1 (Mandatory)**

**Table 1. Control objectives and recommended controls for AI-enabled accounting/audit systems (COSO × ISA 315 × AI Act alignment)** (COSO, 2013; IAASB, 2019)

| **Risk area** | **Control objective** | **Illustrative controls** | **Evidence artifacts (audit-ready)** |
|---|---|---|---|
| Data governance | Ensure data integrity and representativeness | Data lineage mapping; completeness checks; bias testing; access controls | Data dictionaries; lineage diagrams; bias test reports; access logs |
| Model development | Prevent uncontrolled model changes | Model approval gates; version control; independent validation | Change tickets; validation sign-offs; model cards |
| Human oversight | Reduce automation bias and enforce skepticism | Structured challenge protocols; mandatory review for high-impact outputs; override justification | Review checklists; override logs; training records |
| Accuracy/robustness | Maintain performance under real conditions | Drift detection; periodic back-testing; stress tests | Drift dashboards; back-test results; incident reports |
| Transparency | Ensure users understand outputs and limitations | Explanations; disclosure of confidence limits; user guidance | User guides; explainability outputs; limitation statements |
| Security | Protect model and data from tampering | Secure MLOps; access segregation; monitoring for adversarial behavior | Security assessments; IAM logs; penetration test results |
| Monitoring & response | Detect and remediate issues rapidly | KPI thresholds; escalation paths; post-incident reviews | Monitoring logs; escalation records; corrective actions |

*(Cited in text as Table 1.)*

## 4. Discussion

### 4.1 Implications for audit quality and professional skepticism

The core assurance risk is not that AI is “wrong” in a statistical sense; rather, that AI reshapes audit work such that professional skepticism and evidence sufficiency degrade. Under ISA 315 (Revised 2019), auditors must understand the entity’s IT environment and how technology affects risks of material misstatement (IAASB, 2019). When AI systems filter exceptions, prioritize risks, or automate reconciliations, they become part of the system of internal control and must be evaluated as such.

Automation bias undermines both the **risk assessment phase** and the **response phase**. Over-trust in AI outputs can lead to narrower testing, insufficient corroboration, and misinterpretation of anomalies as “false positives” without investigation. Consequently, audit firms should formalize “AI skepticism protocols” analogous to fraud brainstorming: structured challenge of model assumptions, testing of edge cases, and review of override decisions.

### 4.2 Implications for Western Balkan firms in EU-linked supply chains

For firms in the region, AI governance maturity becomes a competitiveness factor. EU customers may request governance assurances, and audit firms may increase scrutiny of AI-enabled controls. A practical implication is that “compliance documentation” should be engineered as a byproduct of good controls (Table 1), not retrofitted at year-end.

### 4.3 Compliance strategy under the EU AI Act

The AI Act’s risk-based approach and phased enforcement create a planning window, but not a reason to delay governance (European Union, 2024; Goodwin, 2024). Firms should adopt a staged roadmap: inventory AI systems, classify risk, implement governance controls, and develop monitoring and documentation. NIST AI RMF and ISO/IEC 42001 can operationalize these steps in an auditable manner (NIST, 2023).

### 4.4 Limitations

This study is framework-based and does not quantify effect sizes of automation bias in specific local audit markets. Future research should include controlled experiments with auditors and accountants in the region and longitudinal studies of AI-enabled control performance.

## 5. Conclusions

AI can materially enhance accounting and audit processes by expanding transaction coverage and improving anomaly detection. However, it also introduces socio-technical risks—particularly automation bias—that can degrade skepticism, weaken internal controls, and jeopardize compliance readiness. Mapping AI risks into COSO and ISA 315 provides an assurance-grounded method to redesign controls (COSO, 2013).

For EU-linked supply chains in the Western Balkans, AI governance is becoming a contractual and assurance expectation even where local law is not yet fully aligned. A practical compliance strategy is to implement lifecycle governance: documented model risk management, robust human oversight, continuous monitoring, and auditable evidence artifacts. The EU AI Act establishes a reference benchmark for these controls, while NIST AI RMF and ISO/IEC 42001 provide actionable frameworks to implement them (European Union, 2024; NIST, 2023).

### Patents

No patentable inventions are claimed. The paper proposes governance, control, and assurance mappings that are intended for broad professional use. Any future implementation into proprietary audit tooling (e.g., automated evidence capture, drift detection dashboards integrated into audit platforms) could involve protectable software configurations, but such developments are not part of this academic manuscript.

### Supplementary Materials

Supplementary materials may include: (i) an AI system inventory template with risk-classification fields aligned to the EU AI Act; (ii) a model card template tailored for accounting/audit tools; (iii) a control-test program for AI-enabled controls (design and operating effectiveness); and (iv) a sample "automation bias mitigation" training module and checklist for audit teams.

### Author Contributions

Harun Tahiri: conceptualization; methodology; regulatory and standards analysis; synthesis of automation bias literature; development of Figure 1 and Table 1; drafting and editing of the manuscript.

### Funding

No external funding was received for this research.

### Institutional Review Board Statement

Not applicable. The study is based on publicly available regulations, standards, and literature and does not involve human participant research.

### Informed Consent Statement

Not applicable.

### Acknowledgments

The author acknowledges the availability of public EU legal texts and international standards that enable evidence-based policy and governance analysis. The author also acknowledges the scholarly community contributing to the emerging literature on AI assurance, algorithm auditing, and human–AI interaction risks.

### Conflicts of Interest

The author declares no conflicts of interest.

### Appendix A

**Audit program excerpt for AI-enabled controls:**

1. Confirm model purpose, owner, and change governance.
2. Validate input data lineage and completeness; test for bias where relevant.
3. Reperform model outputs on a holdout sample; compare to baseline rules.
4. Inspect drift monitoring and incidents; verify corrective actions.
5. Test override logs and reviewer sign-offs; evaluate skepticism protocol adherence.

## Appendix B

**AI Act readiness checklist excerpt:**

- AI inventory completed and risk-classification documented (European Union, 2024).
- Technical documentation and user instructions maintained for each material AI tool (European Union, 2024).
- Human oversight and override protocols implemented, tested, and evidenced.
- Post-deployment monitoring (drift, incidents) operational and reported.
- Supplier due diligence includes AI governance clauses for outsourced models.

## References

1. AICPA & CIMA. (2013). *COSO internal control—Integrated framework (resource overview)*. https://www.aicpa-cima.com/resources/landing/coso-internal-control-integrated-framework

2. Amazon Web Services. (2025). AI lifecycle risk management: ISO/IEC 42001:2023 for AI governance. *AWS Security Blog*. https://aws.amazon.com/blogs/security/ai-lifecycle-risk-management-iso-iec-420012023-for-ai-governance/

3. Artificial Intelligence Act. (2025). *Implementation timeline (community-maintained reference with article mapping)*. https://artificialintelligenceact.eu/implementation-timeline/

4. Cambridge University Press. (2024). Regulation (EU) 2024/1689 (EU Artificial Intelligence Act) (overview note). *International Legal Materials*. https://www.cambridge.org/core/journals/international-legal-materials/article/regulation-20241689-of-the-eur-parl-council-of-june-13-2024-eu-artificial-intelligence-act/64F1F6734F8C66CA3EEA149C9759194E

5. Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework (Executive summary)*. COSO. https://www.como.gov/wp-content/uploads/2021/12/COSO-2013.pdf

6. Daci, E., & Rexhepi, B. R. (2024). The role of management in microfinance institutions in Kosovo: Case study Dukagjini Region. *Quality – Access to Success, 25*(202), Article 22. https://doi.org/10.47750/QAS/25.202.22

7. Deloitte. (2024). *ISO/IEC 42001 standard for AI governance and risk management*. Deloitte Insights. https://www.deloitte.com/us/en/services/consulting/articles/iso-42001-standard-ai-governance-risk-management.html

8. European Parliament Research Service. (2025). *The timeline of implementation of the AI Act*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/772906/EPRS_ATA%282025%29772906_EN.pdf

9. European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act)*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

10. Goodwin. (2024). *EU AI Act timeline: Key dates for compliance*. Goodwin Insights. https://www.goodwinlaw.com/en/insights/publications/2024/10/insights-technology-aiml-eu-ai-act-implementation-timeline

11. International Auditing and Assurance Standards Board. (2019). *ISA 315 (Revised 2019): Identifying and assessing the risks of material misstatement*. IAASB. https://www.iaasb.org/publications/isa-315-revised-2019-identifying-and-assessing-risks-material-misstatement

12. International Organization for Standardization. (2023). *ISO/IEC 42001:2023 Artificial intelligence—Management system*. ISO. https://www.iso.org/standard/42001

13. KPMG. (2024). *ISO/IEC 42001: A new standard for AI governance*. KPMG Insights. https://kpmg.com/ch/en/insights/artificial-intelligence/iso-iec-42001.html

14. Murtezaj, I. M., Rexhepi, B. R., Dauti, B., & Xhafa, H. (2024). Mitigating economic losses and prospects for the development of the energy sector in the Republic of Kosovo. *Economics of Development, 23*(3), 82–92. https://doi.org/10.57111/econ/3.2024.82

15. Murtezaj, I. M., Rexhepi, B. R., Xhaferi, B. S., Xhafa, H., & Xhaferi, S. (2024). The study and application of moral principles and values in the fields of accounting and auditing. *Pakistan Journal of Life and Social Sciences, 22*(2), 3885–3902. https://doi.org/10.57239/PJLSS-2024-22.2.00286

16. Musyoka, F. (2024). Bias and ethics of AI systems applied in auditing: A systematic review. *Journal of Responsible Technology*. https://www.sciencedirect.com/science/article/pii/S2468227624002266

17. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1

18. National Institute of Standards and Technology. (2024). *AI RMF Generative AI Profile* (NIST-AI-600-1). https://www.nist.gov/itl/ai-risk-management-framework

19. Orrick. (2024). *The EU AI Act: Key dates for compliance (timeline)*. https://media.orrick.com/Media%20Library/public/files/insights/2024/the-eu-ai-act-key-dates-for-compliance-timeline-pdf.pdf

20. Rexhepi, B. R., Murtezaj, I. M., Xhaferi, B. S., Raimi, N., Xhafa, H., & Xhaferi, S. (2024). Investment decisions related to the allocation of capital. *Educational Administration: Theory and Practice, 30*(6), 513–527. https://doi.org/10.53555/kuey.v30i6.5233

21. Rexhepi, B. R., Mustafa, L., Sadiku, M. K., Berisha, B. I., Ahmeti, S. U., & Rexhepi, O. R. (2024). The impact of the COVID-19 pandemic on the dynamics of development of construction companies and the primary housing market. *Architecture Image Studies, 5*(2). https://doi.org/10.48619/ais.v5i2.988

22. Romeo, G., & Conti, D. (2025). Exploring automation bias in human–AI collaboration: A review and implications for explainable AI. *AI & Society*. https://link.springer.com/article/10.1007/s00146-025-02422-7

23. Royal Society Open Science. (2024). Towards algorithm auditing: Managing legal, ethical and technological risks. *Royal Society Open Science, 11*(5). https://royalsocietypublishing.org/rsos/article/11/5/230859/92764/Towards-algorithm-auditing-managing-legal-ethical

24. Vecchione, B. (2024). Auditing work: Exploring the New York City algorithmic bias audit regime. *FAccT Conference Proceedings*. https://facctconference.org/static/papers24/facct24-74.pdf

25. White & Case. (2024). *EU AI Act becomes law after publication in the Official Journal: Key compliance implications*. https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal

26. Wieringa, M. (2024). *Automation bias in public sector decision making: A systematic review*. https://www.diva-portal.org/smash/get/diva2%3A1870243/FULLTEXT01.pdf

27. Wilkens, M., Hanelt, A., & Piccinini, E. (2022). What influences algorithmic decision-making? A systematic literature review. *Technological Forecasting and Social Change, 174*, 121249. https://www.sciencedirect.com/science/article/pii/S0040162521008210

28. Wilson, H. J., Daugherty, P. R., & Morini-Bianzino, N. (2017). The jobs that artificial intelligence will create. *MIT Sloan Management Review, 58*(4), 14–16.