

# Artificial intelligence in auditing and compliance in the telecommunications industry: A comparative empirical study of global operators

Ogden Firfov

University American College Skopje, North Macedonia; e-mail: ogden.firfov@uacs.edu.mk

**Abstract:** Telecommunications operators usually operate in highly competitive and highly regulated, data-intensive environments characterized by complex technological IT and NT infrastructure, high level of transaction volumes, and cross-border regulatory obligations. Traditional audit and compliance models — usually and largely based on sample-driven reviews in different time periods — are increasingly insufficient to provide timely and overall assurance. This article analyses the application of Artificial Intelligence (AI) tools in auditing and compliance within six global telecom operators and discusses adoption models, outcomes, and governance challenges.

**KEYWORDS:** INTERNAL AUDIT; ARTIFICIAL INTELLIGENCE; AI GOVERNANCE; COMPLIANCE; TELECOMMUNICATIONS; CONTINUOUS AUDITING

## 1. Introduction

The telecommunications industry is (aside from the banking industry) among the most heavily regulated and technologically complex sectors of the global business and economy. Telco operators manage enormous volumes of commercial transactions, customer data, financial transactions and network events while complying with sector-specific regulation, financial reporting standards, cybersecurity obligations, and data protection regimes such as the General Data Protection Regulation (GDPR). As digitalization accelerates through 5G (and expected 6G in mid-term future), cloud computing, and Internet of Things (IoT) deployments, the scale and complexity of risks confronting telecom operators continue to grow [1]; [2].

Previous research shows that traditional audit and compliance approaches—typically retrospective and sample-based—are increasingly insufficient to address the pace and complexity of digital developments in telecommunications [3]. In response and completely logically, organizations are increasingly exploring Artificial Intelligence (AI) as a means to transform auditing and compliance into continuous, data-driven functions capable of detecting anomalies, predicting risks, supporting proposed improvements and supporting proactive decision-making [4].

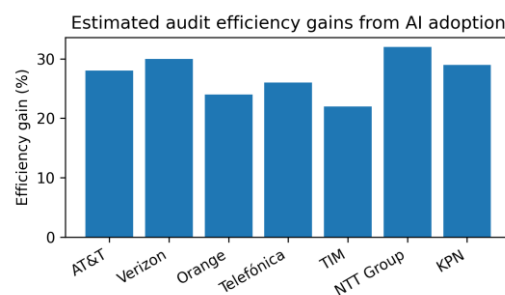
## 2. Literature review and theoretical background

Different authors have an opinion that the auditing landscape is changing with AI, to continuous auditing and complete data populations. The application of AI in auditing has been framed as a transition from conventional assurance models toward continuous auditing and continuous controls monitoring according to [5]. Machine learning enables auditors to analyse complete data populations rather than relying on samples, thereby improving audit coverage and detection capability according to [6]; [7]. Process mining further enhances audit transparency by reconstructing real business processes from event logs, revealing deviations from expected controls [8]; [9]; [10]

Professional bodies acknowledge the transformative potential of AI. The International Auditing and Assurance Standards Board emphasizes that advanced analytics and automation can enhance audit quality, provided that professional judgment and accountability are preserved [4]. Rikhardsson and Yigitbasoglu highlight AI's role in strengthening audit assurance in complex, automated environments [11], while cautioning against overreliance on opaque models and underscoring the importance of explainability and human oversight [12]. It is interesting to note that beside enhanced audit quality, there is also expectation of

increasing audit efficiency per different telco operators due to AI adoption as shown on Figure 1.

**Fig. 1** Estimated audit productivity improvements from AI adoption (AT&T, Verizon, Orange, Telefónica, TIM, NTT Group, KPN)



Explications: Estimated reductions in manual audit work achieved through AI-enabled auditing across the 6 analysed operators.

Beyond audit, artificial intelligence is increasingly deployed in compliance and risk management to monitor regulatory obligations, detect policy breaches, and automate reporting processes [13]. Natural Language Processing (NLP) techniques enable the analysis of large volumes of unstructured textual data, supporting policy and regulatory analysis according to [14]. However, governance and explainability are essential in regulated industries [15]; [16]; [12].

Telecommunications operators are usually a critical environment due to regulatory exposure, complex IT infrastructures, and sensitivity of customer data.

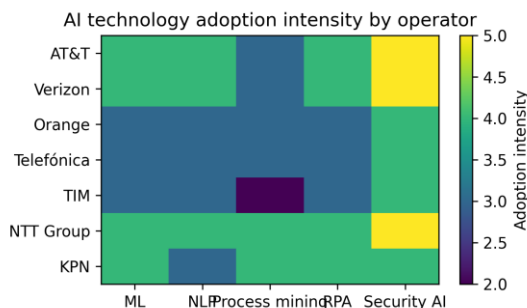
According to European Agency for Cyber Security [17], the deployment of AI in telecommunications can strengthen cybersecurity and fraud detection mechanisms, but simultaneously expands the attack surface and introduces new governance challenges, which aligns with the risk and governance considerations outlined in the NIST AI Risk Management Framework [1].

## 3. Research methodology

This study adopts a qualitative comparative case study methodology suitable for analysing complex socio-technical systems across organizations [18]. Six multinational telecommunications operators with different initial origins were selected: AT&T and Verizon, Orange, Telefónica, Telecom Italia (TIM), NTT Group, and KPN.

Data were collected from publicly available sources including annual reports, sustainability and governance disclosures, regulatory filings, and authoritative industry studies. A structured empirical dataset was developed covering: (1) AI technologies employed; (2) implementation and governance frameworks; and (3) observed outcomes [16].

**Fig. 2** AI technology adoption intensity by operator (including AT&T and Verizon)



Explications: Heatmap of adoption intensity across ML, NLP, process mining, RPA, and security AI (coded low–high) [10].

#### 4. Solution of the examined problem

In order to propose a viable solution, we tried to synthesize the comparative evidence and translate it into an actionable assurance model for large operators. Across the firms which were subject of this paper, the standard pattern is the move from periodic sampling toward population-level testing and continuous monitoring. In telecom, this shift is particularly valuable because critical risk signals (e.g., revenue leakage, roaming anomalies, privileged access misuse, data leakage suspicions) are often rare events embedded in high-volume streams. Machine-learning anomaly detection can detect and surface these outliers earlier than traditional controls testing, provided that data quality and model governance are addressed [4].

From a process perspective, AI-enabled assurance usually follows a three-layer architecture. First, data ingestion consolidates financial, operational, and security telemetry from billing, CRM, network OSS/BSS, identity, and SIEM platforms. Second, analytics and automation implement tests such as: (i) statistical and ML anomaly detection on transactions; (ii) process mining to reconstruct the 'as-is' control flow and detect deviations from the intended process; and (iii) intelligent automation to execute repetitive compliance checks and evidence collection. These approaches are consistent with contemporary continuous auditing models, in which controls are assessed through ongoing evidence streams rather than ad-hoc sampling [5]; [9].

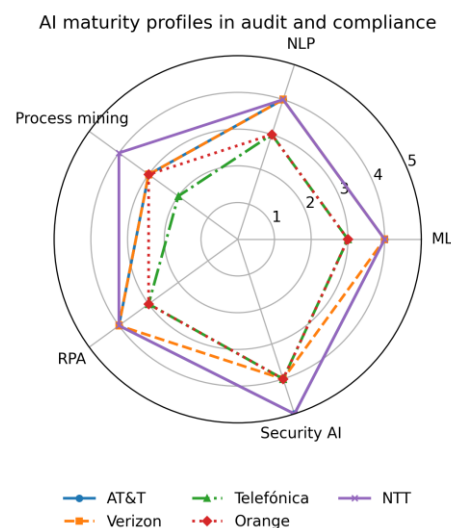
Third, an assurance governance layer operationalises 'human-in-the-loop' decision making. Practically, this means auditors and compliance staff review exceptions flagged by models, validate and confirm root causes, and decide remediation priorities. This is essential because explainability and accountability remain core requirements in regulated environments, especially when automated systems influence compliance decisions [15]; [1].

In comparative terms, the study highlights a clear EU–US contrast, which is somehow expected. EU operators tend to emphasise transparency and regulator-facing traceability, driven by data-

protection enforcement and cross-border supervisory expectations. US operators AT&T and Verizon, operating at extreme scale on a very big single market, typically prioritise operational resilience and security analytics integration, where AI is embedded in monitoring processes and incident response. However, the same governance principles are valid: model controls, audit trails, and clear ownership are required to avoid 'automation bias' and to ensure that AI outputs remain auditable evidence rather than opaque assertions [19].

Figures 1–3 provide a compact representation of these findings. Figure 1 covers outcome-level impact (productivity improvements) which was slightly commented before in section 1. Figure 2 maps technology breadth coverage and general adoption intensity. Figure 3 demonstrates maturity patterns across key AI dimensions in the analysed operators. This three figures together support the conclusion that maturity is not only a function of tools deployed, but of integration into audit workflows and processes and governance controls that make AI outputs reliable for assurance.

**Fig. 3** AI maturity profiles in audit and compliance



Explications: Radar of maturity patterns across Key AI dimensions in the analysed telco companies

It is worth explaining that Figure 3 complements Figures 1 and 2 by illustrating the relative maturity of key AI capabilities across AT&T, Verizon, Telefónica, Orange, and NTT. While efficiency gains (Figure. 1) and adoption breadth (Figure. 2) indicate quantitative and measurable progress, the radar representation highlights qualitative differences in how deeply AI is embedded in audit operations and compliance processes. Operators with higher and more balanced profiles across machine learning, process mining, and security-focused AI can demonstrate greater readiness for continuous auditing and real-time compliance monitoring, provided that governance and explainability controls are in place [5].

#### 5. Results and discussion

In order to interpret the empirical patterns and derive implications for audit and compliance operating models, we came to five conclusions. First and foremost, AI adoption changes the unit of assurance: instead of selecting samples, teams can test entire

populations for defined control assertions (completeness, accuracy, authorization, timeliness). This is particularly relevant for telecom billing, interconnect settlements, roaming traffic settlements, and high-frequency access events (like customer related data issues or transactions). The practical consequence is a reallocation of audit effort—from manual testing to exception investigation, root-cause analysis, and remediation validation [4].

Second and also very important, AI makes stronger the connection between compliance monitoring and security operations. Telecom compliance risks increasingly manifest through cyber issues (compromise of user accounts and passwords, insider misuse, misconfiguration, third-party access). Therefore, audit functions should benefit from integrating with security monitoring and adopting assurance views over SOC (Security Operations Center) processes. Sector guidance emphasises that AI in cybersecurity can improve detection but also introduces new risks (model inversion, data poisoning, automation of attacks), which must be reflected in assurance plans [17]; [20].

Third, the results reinforce that explainability is not a 'nice to have' thing, but it is more and more a pure compliance requirement. When AI supports decisions that affect customers, employees, or regulated reporting, organizations must demonstrate traceability: what data and when they were used, how the model was validated, and how decisions were reviewed and cross checked. Regulatory and policy guidance for trustworthy AI converges on similar control themes: governance, transparency, accountability, and robustness [15]; [1].

Fourth, the study suggests a maturity roadmap for telecom audit functions. Stage 1 focuses on descriptive analytics and automated evidence capture (intelligent RPA). Stage 2 adds anomaly detection and process mining to detect control breakdowns early. Stage 3 integrates predictive risk scoring for audit planning and continuous controls monitoring at scale. Progression toward effective AI-enabled assurance requires sustained investment in data engineering and robust model risk management, rather than a narrow focus on analytics tools alone [21, 22].

Finally, the comparative outcomes should be interpreted quite cautiously. Productivity improvements (Fig. 1) can be achieved quickly in evidence-heavy audits with huge populations, but sustained value depends on how exceptions are handled (or if they are handled at all). If alert volumes are high and false positives are not controlled, AI can shift effort without improving assurance and not much positive gains at the end. Accordingly, operators should track not only efficiency metrics but also quality metrics: precision/recall of alerts, time-to-remediate, recurrence rates, and control failure severity.

## 6. Conclusion

AI-enabled assurance is becoming a necessity in telecommunications (not only in telecommunications but also in other areas of businesses), but real value is realised only when IT systems & technology, governance of processes, workflows and audit and compliance staff skills evolve together. The evidence indicates that technology-enabled continuous auditing can shorten audit cycles, improve anomaly detection, and strengthen compliance responsiveness, particularly when continuous monitoring is integrated into the audit lifecycle [5].

From a corporate governance standpoint, telecom operators should embed and institutionalise a model risk management approach: documented model purpose, training data lineage, validation results, periodic drift monitoring, and clear accountability for overrides. These controls align with emerging international expectations for AI risk management [1].

Future research should mostly focus on the three gaps. (1) Quantitative measurement: longitudinal datasets linking AI adoption to audit outcomes (cycle time, findings the intensity and severity, remediation speed) and to compliance outcomes (incident rates, regulatory findings). (2) Regulatory acceptance: empirical study of how regulators in the telecom environments evaluate AI-generated evidence and what assurance proofs increase trust. (3) Human-AI collaboration: the organizational structure of audit teams, skill profiles of auditors, and training models needed to operationalise AI while preserving professional judgment.

In practical sense, a telecom-ready research design could be a mix: process mining of billing and access-control workflows; supervised and assisted learning for labelled control failures; and qualitative validation through audit committee and regulator interviews afterwards. Such a proposed design would move beyond descriptive adoption claims and provide causal evidence for what works, under which standard and non standard conditions, and at what cost for the telecom companies.

## References

- [1] NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0), Gaithersburg, NIST, 2023.
- [2] Voigt, P. The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer International Publishing, 2017 (Voigt, P., A. Von dem Bussche).
- [3] Vasarhelyi, M.A. Big data in accounting: An overview – Accounting Horizons, vol. 36, 2022, p. 1–22 (Vasarhelyi, M.A., A. Kogan, B.M. Tuttle).
- [4] IAASB The Use of Technology in the Audit of Financial Statements, New York, IFAC, 2020.
- [5] Alles M.G. Drivers of the use and facilitators and obstacles of the evolution of continuous auditing – Accounting Horizons, vol. 29, 2015, p. 439–448.
- [6] Issa, H. Research ideas for artificial intelligence in auditing – Journal of Emerging Technologies in Accounting, vol. 18, 2021, p. 1–20 (Issa, H., T. Sun, M.A. Vasarhelyi).
- [7] Munoko, I. Innovating in Times of Change: The Place for Artificial Intelligence in Auditing – ISACA Journal, vol. 2, 2021.
- [8] van der Aalst, W.M.P. Process Mining: Data Science in Action, Berlin, Springer, 2016.
- [9] Vasarhelyi, M.A. Big data in accounting: An overview – Accounting Horizons, vol. 29, 2015, p. 381–396.
- [10] van der Aalst, W.M.P. Process Mining Put into Context – IEEE Internet Computing, vol. 16, 2012, p. 82–86 (van der Aalst, W.M.P., S. Dustdar).
- [11] Rikhardsson, P. Business intelligence and analytics in management accounting and control – International Journal of Accounting Information Systems, vol. 48, 2023, p. 100598 (Rikhardsson, P., O. Yigitbasioglu).
- [12] Gunning, D. XAI: Explainable artificial intelligence – Science Robotics, vol. 4, 2019, p. 37 (Gunning, D., M. Stefik, J. Choi, T. Miller, S. Stumpf, G-Z. Yang).
- [13] Bai, C. Industry 4.0 technologies assessment – International Journal of Production Economics, vol. 247, 2022, p. 108479 (Bai, C., P. Dallasega, G. Orzes, J. Sarkis).
- [14] Jadeau, J. Enhancing the Availability of Quality Data for Policymaking Using AI – PARIS21 Discussion Paper 19, 2025 (Jadeau, J., M. Fogarassy).

- [15] European Commission Ethics Guidelines for Trustworthy AI, Brussels, European Commission, 2019.
- [16] World Economic Forum The Global Risks Report 2021, Cologne, World Economic Forum - WEF, 2021.
- [17] ENISA Threat Landscape – European Union Agency for Cybersecurity, 2023.
- [18] Yin, R.K. Case Study Research and Applications, Thousand Oaks, Sage, 2018.
- [19] Gunning, D. Explainable artificial intelligence – AI Magazine, vol. 40, 2019, p. 44–58
- [20] ISO/IEC Artificial Intelligence – Risk Management, Geneva, ISO, 2023.
- [21] Grover, V. Creating strategic business value from big data analytics – Journal of Management Information Systems, vol. 35, 2018, p. 388–423 (Grover, V., R. Chiang, T.-P. Liang, D. Zhang).
- [22] Ransbotham, S. Reshaping business with artificial intelligence – MIT Sloan Management Review, vol. 62, 2021, p. 1–17 (Ransbotham, S., D. Kiron, P. Gerbert, M. Reeves).