



P-ISSN:3006-0265 | E-ISSN:3007-4681. Published by the Open University of Kyzylorda

Copyright © Author(s). This is an open-access article distributed under the terms of the [Creative Commons Attribution License \(CC-BY\)](https://creativecommons.org/licenses/by/4.0/).  
<https://bulletin.ouk.kz/index.php/bulletin/index>



## PROFESSIONAL AND LEGAL REGULATION OF THE GOVERNANCE OF ARTIFICIAL INTELLIGENCE USE IN FINANCIAL DISCLOSURE: AN ANALYTICAL STUDY

**Wisam Khalaf Nejres**

University of Kirkuk, Administration & Economics

Corresponding author e-mail: [wisamkhalaf@uokirkuk.edu.iq](mailto:wisamkhalaf@uokirkuk.edu.iq)

**Abstract.** This paper critiques existing professional and legal frameworks that regulate the use of AI for making disclosures within the financial services and invests sector. Artificial intelligence is being used to segment transactions, make estimates, detect anomalies, write narratives and mine corporate reports for details. While there are potential benefits of timely, consistent and analytical capacity in the use of these applications, there are also potential risks on data provenance, bias, opacity, hallucinated content, confidentiality, cyber security and more. The study is qualitative in nature, desk design, and it blends directed document analysis doctrinal legal analysis and functional comparison. The documentary sample includes key materials in international accounting, auditing and ethics plus AI governance, data protection and risk-management. We set out twelve criteria for the analysis to assess the technologies, these relate to data quality, transparency and so on. The study finds that professional regulation presents a very well-developed principles-based framework for integrity, objectivity, competence, due care, confidentiality, evidence, and judgment, but less detail regarding the AI Model on documentation and disclosure. Though legal regulation is better at enforcement, it is usually horizontal and not suitable for the specific features of accounting estimates and financial statements. The integrated and proportional model proposed in the paper, on use-case classification, governance and materiality-based disclosure, management accountability, meaningful human review, algorithmic audit trails and model validation. The key value, however, lies in linking professional duties, legal obligations and technical controls across the full lifecycle of AI-enabled financial disclosure.

**Keywords:** artificial intelligence; financial disclosure; professional regulation; legal regulation; algorithmic governance; auditability; accountability

## Introduction

The digitalization has transformed the architecture of the collection, processing, evaluation and communication of accounting information [1], [2]. The scope of AI applications has extended from basic bookkeeping to pattern recognition, risk scoring, forecasting, reading of documents and drafting of narrative disclosures [3]. Relevance, faithful representation, comparability and timeliness are supported by these capabilities, but the extent to which they contribute depends on data quality, organizational readiness, internal controls and the ability of professionals to evaluate system outputs [4], [5]. Empirical and conceptual research therefore conceptualizes AI as an augmentation technology, with the gains from reporting being contingent, rather than automatic [6].

The governance challenge is especially pertinent to the generation of text for investors using generative AI [7], [8], [9]. Generative artificial intelligence is able to generate fluent and convincing text, but might offer unsupported claims, numerical errors, fake citations, cherry-picking or over-optimism [10]. Also, the detection is not perfect and the reconstruction of authorship and responsibility is difficult [11]. The question is no longer whether a model can produce readable disclosure, but whether the reporting entity can demonstrate that the inputs are reliable, the model appropriate, the human review sound and there is an evidential basis for the output that is approved [12].

Professional regulation addresses this through ethical principles and standards to do with competence, care, confidentiality, judgment, risk assessment and audit evidence [13], [14], [15], [16], [17], [11]. As for a technology, they still apply but many of them were developed with a reporting process in mind where responsibilities and reasoning were more directly linked to identifiable individuals [18]. Machine-learning systems also raise further questions around training data, changing performance, model limitations, dependence on specialists and reliance on technology providers [13], [14]. Therefore, professional requirements have to be translated into procedures for validation, documentation, monitoring and communication with those charged with governance [15], [16].

The legal governance is driven by corporate and securities law, rules on privacy and data protection, obligations on cybersecurity, contract law, civil liability and emerging AI legislation [19], [20]. The European Union AI Act is an example of a risk-based approach and includes requirements for risk management, data governance, record keeping, transparency, accuracy, and security and oversight by humans for systems that fall within its regulated categories [9]. Any personal data processed or exposed during the operation of the model remains subject to the General Data Protection Regulation [21], [10]. International systems from the OECD, NIST and ISO complement binding rules, suggesting lifecycle-oriented methods for identifying and managing AI risk [22], [23].

The issue with research stems from the incompatibility between the speed of AI adoption and the fragmented structure of financial disclosure regulations [24], [3]. Previous research has investigated common themes of adoption outcomes, audit efficiency, ethics, narrative reporting or AI general regulation separately [1]. Less attention is paid to the points where professional duties and legal obligations must intersect to produce demonstrable accountability across the disclosure life cycle [25], [12]. This study addresses this gap by providing an integrated documentary framework for risks, rules, responsible actors, controls and evidences [26].

### Research Problem, Questions, Objectives, and Significance:

The study addresses the question of whether the current professional and legal rules provide a coherent and sufficient basis for controlling AI-assisted financial disclosure [16], [10]. The issue is not a lack of regulation in the broad sense but the fragmentation of relevant duties across accounting and audit standards, ethical codes, AI management frameworks, data-protection rules and sectoral law [20], [14]. Fragmentation can create uncertainty about responsibility for verifying a model's output, the level of documentation required, when to disclose the use of AI, and liability for a materially misleading statement [22], [9].

The main research question is: To what extent and how do professional and legal regulation complement each other in regulating the use of artificial intelligence (AI) technologies in a way that financial disclosure remains reliable, transparent, auditable and accountable? Subsidiary questions include risks to information quality, controls provided by each regulatory domain, residual governance gaps and design of an integrated and proportionate model.

Its aims are to: define AI governance in the light of financial disclosures; clarify the relevant professional and legal obligations; compare the functions and boundaries of the two regulatory fields; evaluate their treatment of data quality, explainability, oversight, auditability, privacy, and responsibility; and develop a common governance framework [12], [16], [22], [10]. The importance is the shift from broad statements about AI efficiency to a control and evidence model that can assist standard setters, regulators, Boards, accountants, auditors, and future empirical researchers [26], [14].

**Table 1.** Summary of prior research and Research Gap

| Study                     | Method                        | Focus                                 | Finding and limitation                                                                 |
|---------------------------|-------------------------------|---------------------------------------|----------------------------------------------------------------------------------------|
| Lehner et al. (2022)      | Normative analysis            | Ethical AI decisions                  | Governance and skills must adapt; disclosure law is not integrated.                    |
| Al-Okaily (2024)          | Survey/PLS-SEM                | AI, data quality, disclosure          | Positive effect; regulation is not the analytical focus.                               |
| Bin-Nashwan et al. (2025) | Survey of 734 professionals   | Accuracy, audit efficiency, asymmetry | Data governance moderates benefits; mainly organisational.                             |
| Chiu (2025)               | Legal analysis                | Generative AI and narrative reports   | Risk travels through the reporting chain; principally legal and narrative.             |
| Alotaibi (2025)           | Design science                | AI-enabled reporting governance       | Proposes control pillars; limited professional–legal integration.                      |
| Yang & Zhou (2025)        | Chinese listed-company data   | Disclosure quality                    | AI improves disclosure quality; rules are not evaluated.                               |
| Agostino et al. (2026)    | Literature review             | Public-sector accountability          | Calls for regulatory oversight and deeper theory.                                      |
| Blankespoor et al. (2026) | Large-sample textual analysis | Generative AI in disclosures          | AI-associated text differs linguistically; detection and attribution remain difficult. |

**Source:** Prepared by the author.

The literature has identified four major streams: effects of AI adoption on reporting and audit results, ethics risks and professional judgment, internal data and model governance, and legal issues surrounding automated or generated disclosure [25], [24], [8], [12], [11]. These streams are increasingly connected, but they still do not provide a unified answer to the governance problem [25]. The observed relationship between AI adoption and reporting quality does not indicate the adequacy of accountability arrangements [1]. Likewise, a professional ethical principle cannot become a legally enforceable duty, and it may not be within the scope of horizontal AI law to determine the evidence required to support a material accounting estimate [11].

Hence the research gap is the absence of an integrated analytical model connecting each AI-related reporting risk to a professional requirement, legal safeguard, designated responsible actor, control

activity and auditable evidence [26], [20], [13], [22], [9]. The measurement of attitudes or adoption [12], unlike the present study, does not fill this gap by examining regulatory architecture. The guidance also differentiates between low impact assistance (such as formatting) and high impact uses involving accounting estimates, impairment analysis, material judgments or investor-facing narrative [12].

## Methods

A qualitative desk-based research design was adopted [27]. It combines directed documentary content analysis, doctrinal legal analysis, and functional comparison [28]. Documentary analysis identifies obligations, safeguards, and evidence requirements in authoritative materials [28]. Doctrinal analysis interprets legal duties, responsibility, and enforcement, whereas functional comparison asks how professional and legal regulation respond to the same governance problem [20], [16]. The combined method avoids a purely descriptive review by connecting the meaning of a rule to its regulatory function and operational consequences [29], [10].

The document population comprises international materials relevant to financial disclosure, professional conduct, auditing, data governance, and AI risk [13], [14], [16], [9]. Purposive selection was used to include the IFRS Conceptual Framework and digital reporting materials, the IESBA Code and technology work, IAASB standards and guidance, the EU AI Act and GDPR, the OECD AI Principles, the NIST AI Risk Management Framework, and ISO/IEC 42001 and 23894 [30], [31], [22], [23]. The most recent available version as of 5 September 2026 was used, while earlier sources were retained when still authoritative or conceptually foundational [13], [14].

The unit of analysis is a provision, principle, requirement, or recommendation addressing data quality, transparency, explanation, traceability, human oversight, professional judgment, confidentiality, cybersecurity, bias, auditability, accountability, or enforcement [29], [22]. Each document was coded against twelve criteria [28], [10]. Treatment was assessed as strong, partial, or weak according to three indicators: clarity of obligation, identification of the responsible actor, and the existence of an evidence or oversight mechanism [9]. These labels are structured qualitative judgments rather than statistical scores [27].

Reliability was strengthened through triangulation across professional, legal, and technical sources; consistent operational definitions; separation of explicit requirements from researcher inference; and a traceable link between conclusions and documents [28], [20], [29]. The design does not measure actual corporate compliance or statistically test control effectiveness [22], [9]. In addition, the legal classification of a reporting application depends upon jurisdiction and intended use [10]. Findings should thus be read as a comparative normative assessment rather than jurisdiction-specific legal advice [20].

**Table 2.** Documentary coding framework.

| Analytical category       | Guiding question                                    | Evidence of strong treatment                                    |
|---------------------------|-----------------------------------------------------|-----------------------------------------------------------------|
| Data quality              | Are provenance, completeness, and bias controlled?  | Source records, validation, testing, representativeness.        |
| Transparency/explanation  | Can the model's role and limitations be understood? | Purpose, version, limits, rationale, proportionate disclosure.  |
| Traceability/auditability | Can the output be reconstructed?                    | Input, output, change, approval, and incident logs.             |
| Human oversight/judgment  | Is review meaningful rather than ceremonial?        | Competent reviewer with authority to challenge and stop.        |
| Privacy/security          | Are data and systems protected?                     | Lawful use, minimisation, access control, encryption, response. |

| Analytical category        | Guiding question                                | Evidence of strong treatment                        |
|----------------------------|-------------------------------------------------|-----------------------------------------------------|
| Accountability/enforcement | Are responsibility and consequences identified? | Named owner, escalation, supervision, and sanction. |

**Source:** Prepared by the author.

## Theoretical Framework:

### AI Across the Financial Disclosure Lifecycle

The study defines AI as machine-based systems which, based on inputs, infer how to generate predictions, content, recommendations or decisions with varying degrees of autonomy [20], [10]. Relevant applications for financial reporting include document extraction, account coding, reconciliation, estimate support, anomaly detection, standard research, and narrative drafting [8]. Predictive systems and generative systems need to be distinguished as the former tend to generate classifications or numerical estimates while the latter are responsible for language or code and present unique risks of unsupported content and unstable responses [7], [32], [9].

The disclosure lifecycle starts with financial and non-financial source data, then goes through classification, measurement, estimation, aggregation, review and drafting, and ends with approval and publication [4], [2]. AI could influence all phases [17]. An early data error may propagate through later processing, and a polished final narrative may obscure weak reasoning [6]. Governance must therefore cover the full information system and link model controls to financial-statement assertions, materiality and the risk of misstatement [13], [14], [30].

Evidence suggests artificial intelligence can reduce information asymmetry and improve reporting accuracy where data and organizational governance are effective [24], [26], [1]. These findings should not be taken as indicators of inherent neutrality [31]. Adoption may be more successful in organizations with stronger resources, controls, skills, and innovation capacity, and effects vary across size, sector, and location [10]. Therefore, governance is a causal condition for benefit, rather than simply an administrative supplement to technology [3].

**Table 3.** AI-enabled financial disclosure lifecycle.

| Source data                         | AI processing                           | Disclosure drafting              | Review and publication             |
|-------------------------------------|-----------------------------------------|----------------------------------|------------------------------------|
| Financial and non-financial records | Classification, measurement, estimation | Statements, notes, and narrative | Human challenge, approval, release |

**Source:** Prepared by the author.

The figure shows that governance is not limited to review of final outcomes [10]. Controls start with legal and reliable data, through model suitability and output testing, to evidence-linked drafting and accountable approval [7], [13], [22], [23], [9]. The more material a communication is, or the more market-sensitive it is, the more robust the documentation, independent challenge and fallback arrangements should be [30].

### Professional Regulation

Professional regulation is applied to accountants and auditors in the form of standards, codes of ethics, guidance, inspection practices and disciplinary arrangements [18], [5]. The IESBA framework requires integrity, objectivity, competence and due care, confidentiality and professional behavior [15], [16], [6]. In its technology work, it has found data governance, cybersecurity, reliance on experts and use of client data to train models and communicate with those charged with governance to be significant issues [15], [16]. Technology does not exempt the professional from ethical responsibility according to these principles [11].

This responsibility is reinforced by the audit requirements to understand information systems, assess the risk of material misstatement, develop appropriate responses and obtain sufficient appropriate evidence [33], [13], [14], [2]. One should not assume that model outputs are reliable simply because they are produced quickly, seem correct, or are produced by a prominent vendor [33]. Provenance, exception handling, model change, access rights and service-organisation dependence have to be

taken into account by professionals [33]. When the logic or evidence under consideration is not available, the limitation in the evidence should influence the audit approach [4], [17].

Professional principles are flexible and technically near to accounting practice, but the implementation of AI-specific is still uneven [10]. There is no standard for the minimum content of a model record, the threshold for disclosure of AI involvement, or the responsibility of a technology provider [12], [22], [9]. Hence, there is a need for leadership from professional regulation on how to translate competence, care and evidence into requirements for model validation, logging, monitoring and escalation, with legal accountability when market information and protected data are affected [14], [15], [16].

## Legal Regulation

AI-enabled financial disclosure is governed by overlapping regimes [9]. Corporate and securities law ensure that information published is accurate and complete, data-protection law regulates the processing of personal information, cybersecurity rules protect systems, contract law regulates the allocation of duties between entities and providers, and civil or administrative liability provides consequences for harm or misleading disclosure [19], [20], [22]. The EU AI Act has a horizontal risk-based structure. Whether a specific reporting tool is regulated as high-risk is determined by its intended purpose and legal classification, and not solely by its accounting importance [21], [10].

In particular, when sensitive or personal data are entered into a cloud service or used for model training, data protection becomes important [7], [34]. Technical and contractual controls should correspond to the principles of lawfulness, purpose limitation, minimization, accuracy, security and accountability [19]. Provider contracts should address data ownership, where data are processed, data retention, how data will be used to train models, the identity of sub-processors, incident notification, audit rights, continuity and exit [32], [22]. Regulating cross-border transfers or downstream processing by an external service can be done only through professional confidentiality [15], [16].

Legal regulation provides enforceability, supervisory authority, sanction and redress but can be broad and slower to adapt than technology [12], [20]. International evidence suggests that most jurisdictions rely heavily on existing financial rules and non-binding AI guidance, with relatively few jurisdictions providing detailed clarification for each financial use case [22], [23], [10]. Therefore, effective governance should adapt existing duties to new systems by means of adaptive professional procedures instead of waiting for a statute that is specifically designed for each accounting application [11], [9].

## Results and Discussion

### Analytical Framework and Findings

#### Risk–Control Mapping

**Table 4.** AI disclosure risks and integrated controls.

| Risk                    | Financial disclosure effect              | Professional control                              | Legal/technical control                                  |
|-------------------------|------------------------------------------|---------------------------------------------------|----------------------------------------------------------|
| Poor or biased data     | Misleading measurement or disclosure     | Source verification and professional challenge    | Data governance, minimisation, quality and bias testing. |
| Generated hallucination | Unsupported statements or references     | Independent review and evidence linkage           | Human oversight, output logs, editorial responsibility.  |
| Model opacity           | Estimate cannot be explained or verified | Suitability assessment and specialist involvement | Purpose, limitation, version, and explanation records.   |
| Model drift             | Performance deteriorates after approval  | Continuous monitoring and revalidation            | Change control, periodic testing, incident management.   |

| Risk                       | Financial disclosure effect                   | Professional control                             | Legal/technical control                                      |
|----------------------------|-----------------------------------------------|--------------------------------------------------|--------------------------------------------------------------|
| Data leakage               | Confidentiality, legal, and reputational harm | Confidentiality and access control               | Lawful processing, security, provider clauses, notification. |
| Automation bias            | Judgment and scepticism are weakened          | Mandatory challenge and human approval           | Authority to intervene and accountable use-case owner.       |
| Provider dependence        | Loss of evidence, control, or continuity      | Evaluation of service provider and expert        | Audit, exit, continuity, portability, and incident rights.   |
| Undisclosed AI involvement | Users misunderstand source or reliability     | Governance communication and material disclosure | Proportionate transparency and publication responsibility.   |

**Source:** Prepared by the author.

The mapping illustrates that none of the major risks is fully mitigated by one regulatory instrument [22], [10]. Ethical objectivity alone cannot detect training-data bias, and a technical bias test is of little use without a responsible professional interpreting the impact on an accounting estimate [16]. Data-protection law may protect personal information, but does not determine whether evidence supports an assumption of impairment [19], [20], [14]. Therefore, governance needs to coordinate professional, legal, contractual and technical measures around the same reporting assertion [9].

## Comparative Adequacy

**Table 5.** Comparative adequacy assessment.

| Criterion               | Professional regulation                               | Legal regulation                             | Integrated assessment                                         |
|-------------------------|-------------------------------------------------------|----------------------------------------------|---------------------------------------------------------------|
| Data quality            | Strong on care and evidence; limited technical detail | Strong for personal data; otherwise variable | Require provenance and testing standard.                      |
| Transparency            | Partial on disclosure of AI use                       | Stronger where a specific duty applies       | Materiality-based AI disclosure rule.                         |
| Explainability          | Implicit in verification and evidence                 | Express for selected regulated systems       | Minimum explanation for material estimates.                   |
| Human oversight         | Strong principles of judgment and responsibility      | Risk-based oversight obligations             | Define meaningful, documented review.                         |
| Auditability            | Strong evidence orientation; weak model-record detail | Logging applies in defined contexts          | Common algorithmic audit trail.                               |
| Privacy/confidentiality | Strong ethical duty                                   | Strong enforceable rights and duties         | Integrated data and provider assessment.                      |
| Responsibility          | Clear for professionals, less so for providers        | Enforceable but fragmented                   | Named owners, contracts, and non-transferable accountability. |
| Adaptability            | Principles and guidance can evolve quickly            | Legislative change is slower                 | Co-regulation with technical standards.                       |

**Source:** Prepared by the author.

Effective governance requires judgment, evidence, competence and ethical conduct [14], [16]. The most effective legal regulation is when there are rights, enforceability, supervision and sanction [12], [10]. According to ISO [22], both differ in the way they set model records, explanation threshold, and disclosure of AI involvement. The right answer is reciprocal translation, such that professional standards translate legal expectations into accounting procedures, and law provides the binding force of safeguards on market integrity and data rights [20].

## Proportionality and Disclosure of AI Use:

According to Blankespoor [8] and the European Parliament & Council [20], a blanket mandate that defines every AI tool will generate immaterial boilerplate and even potentially reveal legitimate confidential information. Three broad levels of governance are identified: low impact assistance, such as formatting in Excel or conducting background research; medium impact use such as anomaly analysis or drafting assistance; and high impact use impacting a material estimate, judgment or a market communication [12], [30], [9]. In situations with significant consequences, thorough documentation and assessment of criteria is essential and must be performed to determine their materiality. This includes purpose, data, limitations, testing, independent challenge, approval, fallback arrangements and the disclosure of technology's role [7], [22].

**Table 6.** Risk-proportionate classification of AI uses

| Low impact                                    | Medium impact                                   | High impact                                                |
|-----------------------------------------------|-------------------------------------------------|------------------------------------------------------------|
| Formatting, translation, preliminary research | Analytics, anomaly detection, assisted drafting | Material estimate, judgment, or investor-facing disclosure |

**Source:** Prepared by the author.

AI-generated financial disclosures should be distinguished from disclosures about the use of AI [8], [10]. The latter is still subject to the usual requirements of recognition, measurement, presentation and faithful representation [20]. The second is relevant where failure to do so would conceal a material source of uncertainty, a significant model dependence or a reporting risk that may affect users' decisions [30], [31]. Disclosure should describe the relevant function and limitation without excessive technical detail [12], [3]. Saying AI was used, period, isn't good enough.

## Allocation of Responsibility

**Table 7.** Accountability allocation.

| Actor                   | Primary responsibility                         | Expected evidence                                     |
|-------------------------|------------------------------------------------|-------------------------------------------------------|
| Board/audit committee   | Risk appetite and oversight                    | Policy, minutes, risk and incident reports.           |
| Financial management    | Integrity and final approval of disclosure     | Judgment memorandum and named approval.               |
| Professional accountant | Care, objectivity, and verification            | Testing, sources, and exception resolution.           |
| Internal audit          | Design and operating effectiveness of controls | Test reports and remediation follow-up.               |
| External auditor        | Risk assessment and audit evidence             | Procedures, technology and expert evaluation.         |
| IT/data science         | Model, data, security, and change control      | Model card, version, performance, change log.         |
| Technology provider     | Contracted performance, evidence, and security | Assurance reports, incidents, audit and exit support. |
| Regulator               | Rules, supervision, and enforcement            | Guidance, inspection, corrective action, sanction.    |

**Source:** Prepared by the author.

External technology does not transfer management's ultimate responsibility for financial disclosure and does not eliminate the professional duties of the accountant or auditor [12], [13], [14]. Collective and ambiguous responsibility should be replaced by a named owner for each use case, a named approver and an escalation route for low confidence, unexpected change or incident [20], [9]. The

entity should be able to obtain sufficient information to validate a material output without breaching provider confidentiality and intellectual property claims [16], [22].

## Proposed Integrated Governance Model

**Table 8.** Integrated governance model for AI-enabled financial disclosure.

| <b>Govern</b>                    | <b>Map</b>                       | <b>Measure</b>                      | <b>Manage</b>                   | <b>Evidence</b>        | <b>Disclose</b>                         |
|----------------------------------|----------------------------------|-------------------------------------|---------------------------------|------------------------|-----------------------------------------|
| Policy, ownership, risk appetite | Purpose, context, affected users | Data, model, bias, robustness tests | Controls, monitoring, incidents | Logs, review, approval | Material information and accountability |

**Source:** Prepared by the author.

The model is composed of six coupled functions [7]. Governance determines policy, defines use cases, assigns ownership and risk appetite [26], [10]. Mapping identifies the accounting purpose, context, users, assertions and potential consequences [20]. NIST [9]. Measurement tests data quality, model performance, bias, robustness and limitations. Management establishes controls, monitoring, change procedures and incident response [22], [23]. Versions, inputs, outputs, tests, changes and approvals are combined. [26] Disclosure helps to know what information is material and who is responsible for publishing this information [26]. The monitoring results are used to inform governance as a part of continuous improvement [26].

The model is predicated on professional standards that require a competent person to verify that the output has a source, is relevant, is not inconsistent with accounting standards and has evidential support before the output is entered into the financial report [14], [16], [9]. Material estimates should be independently challenged and alternatives considered [19], [20]. Legal principles translate into legitimate data use, security, provider controls, transparency, oversight and enforceable documentation [19], [20], [22]. Such construction enables trust to be a matter of provable evidence and not rhetoric [19], [20].

An adequate algorithmic audit trail should include use-case name and owner; model, version and provider; accounting purpose and affected assertions; data sources and dates; operating settings; original output; human amendments; validation procedures and results; exceptions; approvals; incidents; and disclosure decision [7], [12], [22], [9]. Even when using a cloud service, the record can be tracked, and this gives the auditors and the regulators the ability to determine whether the oversight by humans was substantive or only nominal [13], [14], [11].

**Table 9.** Minimum controls by impact level.

| <b>Control</b>        | <b>Low impact</b>   | <b>Medium impact</b>    | <b>High impact</b>                             |
|-----------------------|---------------------|-------------------------|------------------------------------------------|
| Use-case registration | Brief               | Full                    | Full plus governance approval                  |
| Data review           | No sensitive input  | Source and sample check | Comprehensive governance and testing           |
| Output validation     | User review         | Second reviewer         | Independent validation/specialist where needed |
| Model record          | Name and purpose    | Version and limits      | Model card and full audit trail                |
| Monitoring            | Periodic            | Performance indicators  | Continuous drift and incident monitoring       |
| Fallback              | Optional            | Required                | Tested and formally approved                   |
| Disclosure decision   | Usually unnecessary | Materiality assessment  | Documented assessment and                      |

| Control | Low impact | Medium impact | High impact              |
|---------|------------|---------------|--------------------------|
|         |            |               | proportionate disclosure |

**Source:** Prepared by the author.

## Discussion

Results support previous findings that data governance conditions the association between AI use and reporting quality but extend that finding [24], [26], [1]. Reliable data availability is necessary, but not sufficient unless the role of the model is explainable, the process is traceable, a person is responsible for approval and the material technological dependence is considered for disclosure [12]. There may be empirical gains in the quality of reporting, but there may also be unobserved provenance, tone, or verification risk, especially when generative models are involved [8], [3].

The analysis also supports the continued use of human judgment but not ceremonial human approval [22], [9]. For effective oversight, competence, authority, time and access to information are required to challenge, override or stop the system [15], [16]. A reviewer who cannot understand the limitations or find independent evidence cannot make an opaque output reliable reporting just by signing it [13], [14]. Therefore, work design, documentation, training, and resources need to support ethical responsibility [11].

Co-regulatory is the preferred institutional arrangement [31], [10]. Law creates rights, boundaries, oversight, and consequences; professional regulation determines how these expectations are applied in accounting measurement, disclosure, and audit; and technical standards determine lifecycle controls [20], [16], [22], [9]. Greater collaboration among accounting standard setters, securities regulators, data authorities and AI regulators is needed to prevent gaps in regulation and duplicative obligations [10].

The internal impact categories we proposed here should not be confused with statutory classifications provided under the EU AI Act and other jurisdictions [10]. A financial reporting application isn't automatically classified as a high-risk system established by legislation (European Parliament and Council [20]; ISO [22]). Yet, for one which may cause a material misstatement or otherwise undermine market confidence, a more stringent control may be applied by an entity (IAASB [13]; IFRS Foundation [30]). The standards of internal governance should go beyond the legal minimum [9].

## Conclusions and Recommendations

AI does not absolve the reporting entity from its responsibility for financial disclosure, it changes what the entity has to be able to prove [10]. Professional regulation provides the language of ethics, competence, judgment and evidence [14], [16]. Legal regulation offers enforceability, protection of rights, supervision, and sanctions [20]. Technical standards provide lifecycle management tools [9]. No single one is enough [20]. The most critical gaps concern: proportionate disclosure of AI use, model documentation, meaningful oversight by humans, provider assurances, algorithmic audit trails and responsibility allocation [22].

1. Professional standard setters should provide application guidance specifically on AI in accounting estimates, disclosures and audit evidence.
2. Management should maintain a complete inventory of AI use-cases, assign ownership and retain ultimate accountability for any published disclosure.
3. An audit trail of algorithms should be incorporated into the internal control over financial reporting and into the relevant audit documentation.
4. Human review should be grounded in competence, authority, access to evidence and the ability to challenge or stop the system.
5. Contracts with providers should cover training use, confidentiality, data location, sub-processors, incidents, audit rights, continuity and exit.
6. Entities should perform a documented materiality assessment to decide whether to disclose the role, limitation, or uncertainty of AI.
7. Regulators of accounting, securities, privacy, cybersecurity and AI should co-ordinate guidance and supervision.

8. Future research should empirically test the proposed model and test the performance of the model across jurisdictions, sectors and entity sizes.

## References

- [1] S. A. Bin-Nashwan, J. Z. Li, H. Jiang, A. R. Bajary, and M. M. Ma'aji, "Does AI adoption redefine financial reporting accuracy, auditing efficiency, and information asymmetry?" *Computers in Human Behavior Reports*, vol. 17, Art. no. 100572, 2025, doi: 10.1016/j.chbr.2024.100572.
- [2] M. A. Vasarhelyi, A. Kogan, and B. M. Tuttle, "Big data in accounting: An overview," *Accounting Horizons*, vol. 29, no. 2, pp. 381–396, 2015, doi: 10.2308/acch-51071.
- [3] T. Yang and N. Zhou, "Artificial intelligence and the quality of corporate accounting information disclosure," *Finance Research Letters*, vol. 85, Art. no. 108136, 2025, doi: 10.1016/j.frl.2025.108136.
- [4] D. Appelbaum, A. Kogan, and M. A. Vasarhelyi, "Big data and analytics in the modern audit engagement: Research needs," *Auditing: A Journal of Practice & Theory*, vol. 36, no. 4, pp. 1–27, 2017, doi: 10.2308/ajpt-51684.
- [5] J. Kokina and T. H. Davenport, "The emergence of artificial intelligence: How automation is changing auditing," *Journal of Emerging Technologies in Accounting*, vol. 14, no. 1, pp. 115–122, 2017, doi: 10.2308/jeta-51730.
- [6] S. G. Sutton, M. Holt, and V. Arnold, "The reports of my death are greatly exaggerated—Artificial intelligence research in accounting," *International Journal of Accounting Information Systems*, vol. 22, pp. 60–73, 2016, doi: 10.1016/j.accinf.2016.07.005.
- [7] C. Autio et al., *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, NIST AI 600-1. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.AI.600-1.
- [8] E. Blankespoor, E. deHaan, and Q. Li, "Generative AI in financial reporting," *Journal of Accounting Research*, vol. 64, no. 3, pp. 1189–1232, 2026, doi: 10.1111/1475-679X.70050.
- [9] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1. Gaithersburg, MD, USA: U.S. Department of Commerce, 2023, doi: 10.6028/NIST.AI.100-1.
- [10] Organisation for Economic Co-operation and Development, *Regulatory Approaches to Artificial Intelligence in Finance*, OECD AI Papers, no. 24. Paris, France: OECD Publishing, 2024, doi: 10.1787/f1498c02-en.
- [11] O. M. Lehner, K. Ittonen, H. Silvola, E. Ström, and A. Wührleitner, "Artificial intelligence-based decision-making in accounting and auditing," *Accounting, Auditing & Accountability Journal*, vol. 35, no. 9, pp. 109–135, 2022, doi: 10.1108/AAAJ-09-2020-4934.
- [12] I. H.-Y. Chiu, "Using generative artificial intelligence in corporate narrative reporting: Understanding risks within the lens of a reporting chain approach," *Cambridge Forum on AI: Culture and Society*, vol. 1, Art. no. e43, 2025, doi: 10.1017/cfl.2025.10038.
- [13] International Auditing and Assurance Standards Board, *International Standard on Auditing 315 (Revised 2019): Identifying and Assessing the Risks of Material Misstatement*. New York, NY, USA: IFAC, 2019.
- [14] International Auditing and Assurance Standards Board, *Non-authoritative Support Material: Using Automated Tools and Techniques When Identifying Risks of Material Misstatement in Accordance with ISA 315 (Revised 2019)*. New York, NY, USA: IFAC, 2022.
- [15] International Ethics Standards Board for Accountants, *Technology Working Group Final Phase 2 Report*. New York, NY, USA: IFAC, 2022.
- [16] International Ethics Standards Board for Accountants, *Handbook of the International Code of Ethics for Professional Accountants*. New York, NY, USA: IFAC, 2024.
- [17] H. Issa, T. Sun, and M. A. Vasarhelyi, "Research ideas for artificial intelligence in auditing," *Journal of Emerging Technologies in Accounting*, vol. 13, no. 2, pp. 1–20, 2016, doi: 10.2308/jeta-10511.
- [18] International Federation of Accountants, *IFAC 2025 Annual Report: Building Trust and Shaping the Future of the Global Accountancy Profession*. New York, NY, USA: IFAC, 2025.

- [19] European Parliament and Council, "Regulation (EU) 2016/679 (General Data Protection Regulation)," Official Journal of the European Union, L 119, pp. 1–88, 2016.
- [20] European Parliament and Council, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," Official Journal of the European Union, L 2024/1689, 2024.
- [21] Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). Paris, France: OECD, 2019.
- [22] International Organization for Standardization, ISO/IEC 42001:2023, Information Technology—Artificial Intelligence—Management System. Geneva, Switzerland: ISO, 2023.
- [23] International Organization for Standardization, ISO/IEC 23894:2023, Information Technology—Artificial Intelligence—Guidance on Risk Management. Geneva, Switzerland: ISO, 2023.
- [24] M. Al-Okaily, "Artificial intelligence and its applications in the context of accounting and disclosure," Journal of Financial Reporting and Accounting, vol. 23, no. 4, pp. 1387–1401, 2024, doi: 10.1108/JFRA-04-2024-0209.
- [25] D. Agostino, R. P. Lourenço, S. Jorge, E. Bracci, and I. Cruz, "Data science and public sector accounting: Reviewing impacts on reporting, auditing, and accountability practices," Public Money & Management, vol. 46, no. 6, pp. 690–699, 2026, doi: 10.1080/09540962.2025.2529266.
- [26] K. O. Alotaibi, "Developing a comprehensive financial reporting governance framework using AI techniques," Engineering, Technology & Applied Science Research, vol. 15, no. 6, pp. 29202–29207, 2025, doi: 10.48084/etasr.14202.
- [27] M. Schreier, Qualitative Content Analysis in Practice. London, U.K.: SAGE, 2012.
- [28] G. A. Bowen, "Document analysis as a qualitative research method," Qualitative Research Journal, vol. 9, no. 2, pp. 27–40, 2009, doi: 10.3316/QRJ0902027.
- [29] K. Krippendorff, Content Analysis: An Introduction to Its Methodology, 4th ed. Thousand Oaks, CA, USA: SAGE, 2018.
- [30] IFRS Foundation, Conceptual Framework for Financial Reporting. London, U.K.: IFRS Foundation, 2018.
- [31] IFRS Foundation, IFRS Accounting Taxonomy 2025. London, U.K.: IFRS Foundation, 2025.
- [32] International Organization for Standardization, ISO/IEC 22989:2022, Information Technology—Artificial Intelligence—Concepts and Terminology. Geneva, Switzerland: ISO, 2022.
- [33] M. G. Alles, "Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession," Accounting Horizons, vol. 29, no. 2, pp. 439–449, 2015, doi: 10.2308/acch-51067.
- [34] National Institute of Standards and Technology, Cybersecurity Framework (CSF) 2.0, NIST CSWP 29. Gaithersburg, MD, USA: U.S. Department of Commerce, 2024, doi: 10.6028/NIST.CSWP.29.