Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

Digital Trust in Financial Reporting: A Review of Deepfakes, Synthetic Evidence, and AI Generated Corporate Communications

[1]Boluwatife Gabriel Jesutoye, [1]Sodeeq Ipadeola Olalekan, [2]*David Chinonso Anih, [3]Ahmed Oladapo Olaneye & [4]Oyewole Abdulateef Ojora

[1]Information Security Department, INHAF Ltd, Greater Manchester, UK
[2]Federal University Wukari, Taraba, Nigeria
[3]Department of Computer Science, Faculty of Science, Lagos State University, Nigeria
[4]Senior Audit Associate, Ernst & Young, Nigeria
*Corresponding Author's E-mail: anih.david@fuwukari.edu.ng

Abstract: Digital trust has become a central concern in financial reporting as artificial intelligence, deepfakes, synthetic evidence, and AI generated corporate communications increasingly shape how information is prepared, verified, disclosed, and interpreted. This review examines the evolving relationship between reporting integrity and digital authenticity, with particular attention to accounting, external audit, internal control, board oversight, and regulatory response. Drawing on peer reviewed journal studies published between 2023 and 2026, the review synthesizes empirical and conceptual evidence from accounting, auditing, information systems, governance, cybersecurity, and artificial intelligence research. The literature indicates that AI can improve reporting efficiency, readability, and analytical capacity, but it can also intensify bias, transparency concerns, and information asymmetry when governance is weak. Deepfakes and synthetic evidence present an immediate threat because audio, video, image, and text forgeries can imitate legitimate records, impersonate authority, and contaminate audit trails. At the same time, AI assisted drafting can enhance clarity and consistency in annual reports, earnings narratives, sustainability disclosures, and investor communications, yet it may also weaken authenticity, signal detachment, and reduce stakeholder trust when disclosure appears overly automated or strategically polished. The review further shows that digital trust is not restored by technology alone. Effective protection requires a coordinated framework built on provenance tracking, content authentication, human oversight, and enterprise level controls. Technical tools such as metadata retention, content credentials, timestamps, blockchain supported traceability, and workflow logging can strengthen verification, but these measures must be complemented by accountable approval structures, professional skepticism, and clear disclosure policies. The evidence also suggests that regulatory responses should distinguish among types of AI use, the timing of disclosure, and the level of materiality involved. Overall, the manuscript argues that digital trust in financial reporting is fundamentally a governance issue. Future research should prioritize multimodal deepfake detection, audit procedures for synthetic evidence, and cross national studies on AI oversight and transparency.

Keywords: Digital trust, financial reporting, artificial intelligence, deepfakes, synthetic evidence, provenance, audit governance, disclosure quality, corporate communications.

I. INTRODUCTION

Digital trust in financial reporting now depends not only on whether the numbers are accurate, but also on whether the surrounding narrative, supporting evidence, and digital media can still be trusted as authentic. Recent evidence shows that artificial intelligence adoption can improve the readability and accuracy of annual report disclosures by strengthening internal information processing and management efficiency, while broader accounting scholarship finds that AI can accelerate large scale data analysis, support reporting and auditing tasks, and reduce human error [1-3]. At the same time, listed firms are increasingly using AI narratives in annual reports and blending assertive and defensive impression management to shape legitimacy claims and stakeholder perception, which means corporate communication is now about both disclosure quality and perception management [4].

Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

The risk side of this shift is equally important. A systematic review of AI in auditing identifies bias, transparency, accountability, and data dependence as major concerns, and it recommends human oversight, representative testing, periodic system audits, and governance safeguards to preserve trust [5]. Deepfake research adds a more immediate warning by showing that synthetic audio, video, and text can be used for financial fraud and that an effective response requires provenance tracking, watermarking, explainable AI, and cross sector standards such as C2PA [6]. Audit research also suggests that advanced technology and automation are becoming more embedded in assurance work, but that regulation, skills, and ethics will determine whether digitization strengthens or weakens confidence in audit quality. Taken together, these findings imply that digital trust in financial reporting is now a governance problem as much as a technical one: the central challenge is to preserve the authenticity of evidence, the credibility of corporate communications, and the reliability of audit judgments in an environment where machine generated content can imitate reality with increasing plausibility [5-7].

Accordingly, this comprehensive review examines how deepfakes, synthetic evidence, and AI generated corporate communications reshape the preparation, verification, interpretation, and governance of financial reports, with particular attention to implications for accounting, external audit, internal control, and board oversight.

II. METHODS

2.1 Scope and Evidence Base of the Review

This comprehensive review draws on an interdisciplinary body of literature examining the changing nature of trust in financial reporting in an increasingly digital and AI-enabled environment. The evidence base brings together research from accounting, auditing, corporate governance, information systems, cybersecurity, artificial intelligence, and digital communication because the integrity of contemporary financial reporting is no longer determined solely by the accuracy of accounting records. It is also influenced by the technologies used to generate, process, communicate, verify, and preserve reporting information. Recent studies indicate that artificial intelligence can strengthen reporting efficiency, analytical capability, and information processing, while simultaneously introducing concerns relating to bias, transparency, accountability, and the reliability of digitally generated evidence [8-10].

The review therefore considers digital trust as a broad reporting-quality issue rather than as a narrowly technological concept. Particular attention is given to the authenticity of corporate information, the traceability of digital content, the reliability of audit evidence, the credibility of AI-assisted disclosure, and the ability of stakeholders to distinguish legitimate information from manipulated or synthetically generated material. This perspective is important because deepfakes, synthetic documents, AI-generated narratives, and other forms of fabricated digital content can increasingly resemble legitimate corporate communication. At the same time, AI-enabled reporting tools may improve clarity and consistency, creating a dual effect in which the same technologies that enhance communication can also create new opportunities for deception or strategic manipulation [8-10].

The evidence considered in this review consequently spans both the risks and the potential benefits associated with digital transformation in financial reporting. Empirical studies concerning AI adoption, reporting quality, auditing, trust, and information asymmetry are considered alongside emerging research on synthetic media, content authenticity, digital provenance, and verification mechanisms. This broader evidence base makes it possible to examine digital trust across the entire reporting chain, from the creation and preparation of information to its disclosure, independent verification, interpretation, and ultimate use in economic decision-making [8-10].

Rather than treating these strands of literature as isolated areas, the review brings them together around a common question: how can confidence in financial information be maintained when the tools used to create and communicate that information are themselves capable of producing highly convincing synthetic content? This integrated perspective allows the review to identify areas of convergence as well as points of tension within the existing literature. It also highlights the fact that technical safeguards alone may not be sufficient. Trust ultimately depends on the interaction between technological controls, transparent disclosure, human judgment, organizational accountability, professional skepticism, and governance arrangements [8-10].

The review places particular emphasis on recent evidence while retaining earlier contributions where they remain important for establishing theoretical or conceptual foundations. Peer-reviewed empirical research is given substantial weight because evidence concerning actual reporting practices, audit responses, stakeholder perceptions, disclosure behaviour, and governance outcomes provides a stronger basis for understanding the practical consequences of AI and synthetic media than conceptual discussion alone. Studies from adjacent disciplines

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

are also considered where they provide relevant insight into authenticity, provenance, trust formation, misinformation, or digital verification. This is especially important for an emerging subject such as digital trust, where important developments may appear first in information systems, cybersecurity, communication, or AI scholarship before becoming established within accounting research [8-10].

Overall, the evidence base is structured to support a holistic examination of how deepfakes, synthetic evidence, and AI-generated corporate communications are reshaping the foundations of confidence in financial reporting. By integrating these interconnected strands of evidence, the review moves beyond asking whether AI improves or threatens reporting quality and instead considers the conditions under which digital technologies can strengthen efficiency without undermining authenticity, accountability, evidentiary reliability, and stakeholder trust [8-10].

Table 1 explains how the literature search was built across accounting, auditing, governance, AI, cyber risk, and digital trust sources. It captures the databases, keywords, Boolean logic, date range, language, document types, and inclusion priorities used to guide the review.

Table 1: Search strategy matrix

Search element	Suggested contents	Citation(s)
Databases and repositories	Scopus, Web of Science, ScienceDirect, Emerald Insight, SpringerLink, Wiley Online Library, JSTOR, Google Scholar	[8-10]
Core keyword blocks	Digital trust, financial reporting, audit evidence, deepfake, synthetic evidence, AI generated communication, provenance, authenticity, investor trust	[8-10]
Boolean logic	Deepfake OR synthetic media OR AI generated content; provenance OR authenticity OR verification; financial reporting OR disclosure OR audit evidence	[8-10]
Date range	2023 to 2026	[8-10]
Language	English	[8-10]
Document types	Empirical journal articles, field studies, experiments, interviews, and early view papers	[8-10]
Inclusion priority	Accounting, auditing, governance, AI, cyber risk, disclosure quality, provenance, and trust studies	[8-10]

This table summarizes the review search design, including databases and repositories, core keyword blocks, Boolean combinations, date range, language, document types, and inclusion priorities. Abbreviations: AI = artificial intelligence; OR = Boolean search operator; AND = Boolean search operator; Scopus and Web of Science are database names.

2.2 Conceptual Foundations of Digital Trust in Financial Reporting

Digital trust in financial reporting can be understood as the confidence that users place in digitally produced or digitally mediated reporting content because it is perceived as authentic, traceable, and reliable enough to support decisions. In this setting, trust is not just a general feeling. It is tied to whether the content can be traced back to an accountable source, whether its production path is visible, and whether the communication process gives users enough reason to rely on it. Empirical trust research shows that trust in digital environments is strongly shaped by transparency, user expectations, design quality, and the perceived legitimacy of the system producing the content [11-13].

A useful distinction is between trust and trustworthiness. Trust refers to the willingness of a user, investor, auditor, or regulator to rely on a reporting artifact, while trustworthiness refers to the properties that make that reliance reasonable. In financial reporting, trustworthiness depends on authenticity, provenance, control, and evidentiary reliability. The study of AI powered digital agents shows that transparency and design quality can raise trust when users can understand what the system is doing and why it appears credible [12]. At the same time, a provenance based approach demonstrates that users rely more confidently on records when they can see how transformations occurred, who made them, and what form changes took place along the way [13]. For reporting systems, that implies that trust is strengthened not by appearance alone, but by an inspectable chain of production.

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

Authenticity is central to that chain. In financial reporting, authenticity means that a claim, narrative, image, file, or confirmation is genuinely associated with the entity it purports to represent. Provenance adds the next layer by documenting the origin and transformation of the item over time. Evidentiary reliability then asks whether the item can reasonably support an assertion in the reporting process. Recent trust research on generative AI shows that disclosure of AI use can reduce trust when it triggers concerns about typicality, commitment, and authenticity [11,12]. That matters for accounting because a report can become less persuasive not only when it is false, but also when stakeholders doubt how it was made.

The reporting chain in digital trust runs from content creation to verification, disclosure, user reliance, and assurance. Content creation may involve humans, AI, or a hybrid process. Verification checks whether the content matches known records, metadata, approvals, and source systems. Disclosure tells users what role AI or automation played. User reliance then occurs when investors, lenders, analysts, auditors, or regulators interpret the content as decision useful. Assurance comes last, either through internal controls, external audit work, or technical authentication tools. Studies of trust in digital platforms, AI enabled agents, and provenance visualization all suggest that each link in this chain matters because trust breaks down quickly once users cannot see how a digital artifact was produced or whether it has been altered [11-13].

Table 2 defines the central ideas that frame the review. It lays out the working meanings of digital trust, deepfake, synthetic evidence, AI generated communication, provenance, authenticity, and evidentiary reliability.

Table 2: Key concepts and working definitions

Concept	Working definition for this review	Citation(s)
Digital trust	The willingness to rely on digitally produced or digitally mediated reporting content because it appears authentic, traceable, and decision useful	[11,12]
Deepfake	AI generated or AI altered audio, video, image, or text content that imitates a real source deceptively	[11,12]
Synthetic evidence	Fabricated or manipulated records presented as support for an accounting, audit, or compliance claim	[11,12]
AI generated communication	Corporate text or media created or materially assisted by AI for disclosure, publicity, or investor communication	[11]
Provenance	The documented origin of a record and the sequence of its transformations	[13]
Authenticity	The quality of being genuinely attributable to its claimed source and production process	[11,12]
Evidentiary reliability	The extent to which a digital item can be safely used to support an accounting or assurance assertion	[13]

This table presents the main concepts used in the review and gives a brief working definition for each one. Abbreviations: AI = artificial intelligence. Deepfake, provenance, authenticity, and evidentiary reliability are written out in full in the table.

2.3 Deepfakes and Synthetic Evidence as Threats to Reporting Integrity

Deepfakes now matter for financial reporting because they can imitate real people, real transactions, and real documents across audio, video, image, and text formats. The latest deepfake literature shows that the technology is no longer confined to face swapping or video forgery. It includes speech cloning, partial fake speech, manipulated images, and multimodal content designed to look persuasive enough for operational deception or fraud [14-16]. For accounting, the risk is not limited to public misinformation. It extends to internal confirmations, board communications, approval records, customer instructions, and supporting documents that may be used in the audit trail.

Synthetic evidence is especially dangerous because it can sit inside ordinary reporting routines. A manipulated invoice, altered approval email, fabricated bank confirmation, or cloned voice message can appear normal enough to bypass manual review unless controls are strong. The deepfake literature shows that the persuasive power of such content is amplified when it exploits human expectations, authority cues, and urgency signals [16]. The case based analysis of deepfake influence tactics shows that manipulation often works through social persuasion patterns rather than through technical realism alone, which means that

Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

fraud prevention must address both human psychology and media forensics [16]. In the reporting context, that translates into a higher risk of impersonation, false authorization, and unsupported assertions.

A second threat is the weakening of audit evidence. Auditors rely on the quality of evidence, but deepfakes undermine the assumption that a record is what it claims to be. The deepfake detection literature increasingly emphasizes explainability because detection systems themselves must be transparent if they are to support trust in high stakes settings [15]. That is relevant to assurance, where a black box detector is not enough if the auditor cannot explain why a document, call recording, or video clip was flagged. In the same way, the partial fake speech literature shows that even incomplete or strategically edited audio can be enough to create a harmful false impression in real world conditions [16].

The fraud pathway is often incremental. First, a fraudster establishes a believable identity or channel. Next, the fraudster uses synthetic media to create pressure or legitimacy. Then the fabricated content is inserted into a control process, a confirmation workflow, or a management communication route. Finally, the false content affects reporting judgments, audit procedures, or internal approvals. Deepfake research indicates that these attacks are becoming more practical because they can be targeted, fast, and persuasive at low cost [14-16].This makes the reporting chain vulnerable not just to one major forged event, but to repeated micro manipulations that reduce confidence in the whole evidentiary system.

Table 3 explains how synthetic media can disrupt reporting and audit trails. It classifies the main threat types by reporting channel, likely misuse, and accounting or audit implication.

Table 3: Typology of deepfake and synthetic evidence risks

Threat type	Reporting channel affected	Likely misuse	Accounting or audit implication	Citation(s)
Audio deepfake	Management calls, approval messages, confirmation requests	Voice impersonation for unauthorized instruction	False authorization and weakened control reliance	[16]
Video deepfake	Board messages, public statements, crisis communications	Fabricated executive appearance or statement	Reputational harm and misleading disclosure	[14,15]
Image manipulation	Receipts, product evidence, inventory or asset images	Altered visual support for transactions	Unsupported evidence and valuation risk	[14]
Document forgery	Invoices, contracts, confirmations, internal memos	Fake support for entries or balances	Audit evidence contamination	[14-16]
Multimodal synthetic evidence	Entire reporting packets or disclosure bundles	Coordinated fraud across channels	Higher detection difficulty and greater assurance risk	[15,16]

This table classifies the major forms of synthetic evidence risk, including audio, video, image, document, and multimodal attacks. Abbreviations: AI = artificial intelligence; audit = assurance review of financial records; the table itself spells out the channel, misuse, and implication categories.

2.4 AI Generated Corporate Communications and Disclosure Quality

AI generated corporate communication has become a serious reporting issue because companies increasingly use AI assisted drafting for annual reports, press releases, earnings narratives, sustainability statements, and investor messages. The main benefit is efficiency. AI can accelerate drafting, reduce repetitive work, and improve surface level readability. But empirical evidence shows that communication quality is not simply a matter of faster production. What matters is whether the content is clear, credible, and aligned with underlying performance [17-19]. In other words, AI can improve form while still weakening trust if it hides uncertainty or introduces overconfident language.

Readability and tone are especially important in reporting. International evidence from integrated reports shows that more

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

readable and optimistic tone is associated with higher market value of equity, suggesting that disclosure style influences investor interpretation and not merely communication aesthetics [17]. That finding matters for AI generated drafting because large language models can easily create polished prose, but polish does not guarantee substance. If AI improves fluency without improving accuracy, it may increase persuasion while lowering informational quality. That risk is even greater when disclosures are drafted to sound authoritative but are not carefully anchored in source data.

The trust literature also warns that disclosure itself can create a penalty. Research on AI disclosure shows that simply revealing AI involvement can reduce trust because people infer lower authenticity, weaker commitment, and lower legitimacy [18]. A related consumer study found that AI generated content disclosures reduced engagement, not because people thought the content was necessarily low quality, but because disclosure weakened the emotional and relational connection with the creator [19]. In financial reporting, the same pattern may appear when investors read a report that is technically accurate but seems overly automated or detached from human judgment. That means firms face a difficult balance: hiding AI use can undermine transparency, but disclosing it without careful framing can also reduce trust.

There is also a strategic risk. AI may be used to create disclosure that is technically compliant yet subtly evasive. It can smooth over uncertainty, reduce direct language, or amplify favorable sentiment while burying negative signals. The sustainability reporting literature shows that AI adoption can reshape reporting practices toward more data driven and potentially more independently structured disclosure, but it also signals that AI becomes part of the reporting architecture rather than merely a writing tool [19]. For corporate reporting, that means AI should be treated as a governance issue, not only a communications aid.

The broader implication is that disclosure quality must be measured at two levels. At the surface level, AI can raise readability, consistency, and stylistic polish. At the substantive level, however, the report must still faithfully represent performance, risk, uncertainty, and stewardship. The stronger empirical studies in this area show that readability, tone, AI disclosure, and trust are linked in ways that can either support or weaken market interpretation [17-19]. A comprehensive review therefore needs to track not only whether AI is used, but how its use alters the truthfulness, interpretability, and perceived sincerity of the final communication.

Table 4 discusses how AI can improve style while still affecting trust and substance. It brings together evidence on readability and tone, AI disclosure and trust, and AI in sustainability reporting to show the dual effect of AI on report quality.

Table 4: Evidence on AI generated disclosures and report quality

Study focus	Method	Main finding	Implication for financial reporting	Citation(s)
Integrated report readability and tone	Cross country empirical analysis of firm year observations	More readable and optimistic tone is linked to higher market value of equity	AI drafting may improve style, but tone must be anchored in performance reality	[17]
AI disclosure and trust	Content analytic study, vignette experiment, and replication	Disclosing AI use lowers trust through legitimacy concerns	Disclosure policy should be explicit, but also carefully contextualized	[18]
AI in sustainability reporting practice	Empirical practice oriented analysis	AI can reshape sustainability reporting and intellectual capital disclosure	AI should be governed as part of the reporting system, not treated as a neutral tool	[19]

This table summarizes how AI affects disclosure quality through readability, tone, trust, and sustainability reporting practice. Abbreviations: AI = artificial intelligence; report quality refers to the clarity, credibility, and substantive value of disclosure.

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

2.5 Governance, Provenance, and Regulatory Responses

The governance response to digital trust risk has to work at three levels: content authentication, human oversight, and enterprise controls. Content authentication asks whether a file, message, image, or disclosure can be verified as genuine. Human oversight asks whether a responsible person reviewed, approved, and signed off on the content before publication or use. Enterprise controls ask whether the entire reporting system has built in safeguards against manipulation, unauthorized generation, and hidden editing. Recent accounting and information systems studies show that blockchain, provenance design, and governance aligned architectures can support reliable information exchange, but they also show that technical solutions must be complemented by organizational controls and trust arrangements [20-22].

The accounting literature on blockchain adoption shows that the main challenges are often not purely technical. They involve evidence quality, ownership, valuation, and the difficulty of obtaining trustworthy support for reported balances and transactions [20]. In practice, blockchain can help create immutable records, but it does not automatically solve the problem of whether input data were truthful in the first place. That is why governance matters. If the original data are false, an immutable ledger simply preserves the falsehood more efficiently. So the real value of blockchain in financial reporting lies in improving traceability, control visibility, and assurance readiness rather than in replacing judgment.

Provenance tools offer a second response. Research on provenance visualization shows that documenting the origin of records and the sequence of transformations can make hidden decisions visible and improve transparency, rigor, and ethical interpretation [20]. Although that study is not about accounting, its logic transfers directly to financial reporting systems because reports also pass through multiple transformation steps before users see them. A provenance layer can show who created the content, which systems modified it, what approvals occurred, and whether AI assisted any stage. That kind of traceability becomes especially valuable when synthetic evidence or AI generated text is involved.

A third response is to design trust enabling workflows that reduce opportunism and prevent information manipulation. A blockchain based information sharing study shows that reliable interorganizational exchange can be supported when a system is designed to permit truthful sharing without exposing unnecessary sensitive data [21]. Another design science study shows that blockchain systems for interorganizational exchange can be built to support trust, coordination, and value sharing when governance tradeoffs are addressed explicitly [22]. For financial reporting, those insights suggest that digital trust should be engineered into the workflow itself through approved templates, timestamped logging, segmented permissions, dual sign off rules, and traceable content creation pathways.

At the regulatory level, the key issue is transparency without overload. A balanced regime should require firms to label material AI involvement where it affects disclosure quality or evidence reliability, while also requiring internal records that show how outputs were checked. Human oversight should remain mandatory for material disclosures, and AI generated evidence should be treated as high risk unless corroborated by independent records. The direction of the literature suggests that trust is not restored by technology alone. It is restored when technology, governance, and responsibility work together across the full reporting chain [20-22].

Figure 1 presents a six stage workflow showing how content moves from human or AI creation through provenance capture, internal review, authenticity checking, disclosure, and external assurance. It also highlights the feedback loops and foundational principles that support trustworthy and accountable user reliance.

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

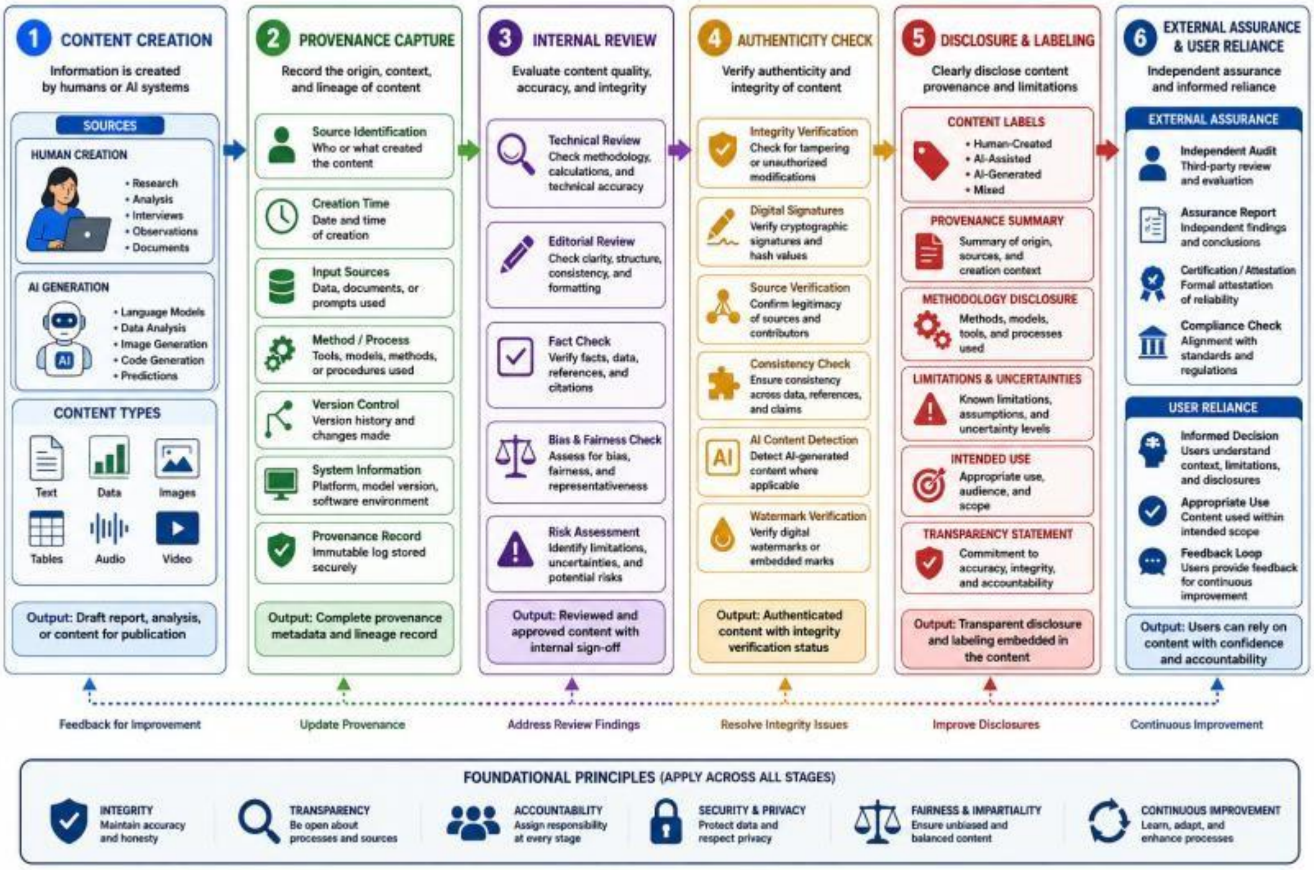

Figure 1: Transparent Workflow for Content Creation, Verification, Disclosure, and User Reliance [20-22]

Schematic of the content governance pathway from creation to user reliance, including source capture, version control, technical and editorial review, authenticity verification, labeling, and independent assurance. Abbreviation: AI, artificial intelligence.

III. RESULTS AND DISCUSSION

3.1 Deepfakes and the Erosion of Evidentiary Reliability

Synthetic media has moved far beyond the novelty stage and now represents a direct challenge to the evidentiary foundations of financial reporting. In practice, the danger is not only that deepfakes can look or sound convincing, but that they can borrow the authority of familiar formats, such as a chief executive's voice note, a boardroom video call, a signed approval screenshot, or an apparently routine documentary attachment. A recent experiment on deepfake speech recognition showed that when people were exposed to synthetic audio without warning, they struggled to distinguish it from genuine speech, even when the task was designed to mimic a realistic encounter with the false material [23]. For accounting, this matters because confirmations and attestations are often treated as strong evidence precisely because they appear direct and unmediated. Once the voice, face, or recorded statement can be fabricated at scale, the evidentiary value of "hearing it from the source" or "seeing it on video" becomes much less secure.

The problem is even sharper for voice cloning, because audio evidence often carries a false sense of intimacy and immediacy. A 2025 study found that voice clones can sound realistic enough to preserve the impression of naturalness, but that this realism should not be mistaken for true hyperrealism, meaning that the surface quality of the voice does not guarantee authenticity [24]. The same study also suggests that familiarity changes detection, because people who know the original speaker better may be more sensitive to subtle cues than strangers are. That distinction is important for accounting workflows. An auditor or controller who receives a voice message from an unknown vendor, client, or executive may be less able to detect fraud than someone who knows the speaker well. In other words, synthetic audio weakens the assumption that direct oral communication is automatically reliable,

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

especially when it is used to authorize payments, explain unusual adjustments, or pressure staff into bypassing normal controls.

This risk is not theoretical. Real world deepfake attacks increasingly target situations in which speed, authority, and uncertainty intersect. A study on partial fake speech attacks found that both humans and machines can be deceived by mixed real and synthetic speech, and that current defenses remain insufficient against this type of manipulation [25]. That finding is particularly relevant to finance because partial manipulation is often enough to corrupt a decision. A short edited instruction from an apparent CFO, a clipped voice clip inserted into a recorded call, or a synthetic line embedded inside a larger authentic message may be sufficient to trigger a mistaken transfer, an inappropriate confirmation, or a false belief that third party verification has already occurred. For fraud detection, the implication is sobering. Traditional skepticism often assumes that fake evidence will be visibly clumsy, but modern synthetic content may be polished, context aware, and strategically limited to just enough of the message to pass casual scrutiny.

Table 5 shows how these evidentiary failures can travel through the reporting process. The common thread is that synthetic media weakens the link between form and truth. Once that link weakens, every downstream user, including preparers, auditors, directors, lenders, and regulators, has to spend more time validating provenance rather than simply reading the content as evidence. That shift increases the verification burden and makes professional skepticism not just prudent, but structurally necessary.

Table 5: Evidence pathway analysis of deepfake related reporting risks

Source of evidence	Risk introduced	Control weakness	Likely consequence	Citation(s)
Video or audio confirmation from an executive	Impersonation of authority through synthetic voice or face	Reliance on appearance or voice alone	False approval, unauthorized payment, or misleading board instruction	[25]
Third party voice or video verification	Mixed real and synthetic content that appears authentic	No systematic authenticity check before reliance	Fraudulent assurance and delayed detection	[25]
Documentary evidence presented as a recording or clip	Manipulated context that changes meaning without obvious editing marks	Spot checking without provenance validation	Contaminated audit trail and weak evidential value	[25]

This table shows how different evidence sources can be manipulated and how that manipulation affects reporting reliability. Abbreviations: AI = artificial intelligence; the table uses evidence source, risk introduced, control weakness, and likely consequence as its core columns.

3.2 Synthetic Documents, Internal Controls, and Audit Procedures

Synthetic documents extend the deepfake problem into the documentary core of accounting. Invoices, purchase orders, bank letters, contracts, approvals, and management correspondence no longer need to be physically forged in the old sense. They can now be generated or altered digitally with enough consistency in layout, language, and metadata to resemble legitimate records. The move to remote work and digitized workflows during and after the pandemic exposed how heavily internal audit depends on evidence moving through screens, portals, email chains, and collaboration tools rather than through in person inspection. A field study of internal auditing during COVID 19 showed that remote work forced internal auditors and audit teams to conduct their work differently, making improvisation and adaptation part of the audit process itself [26]. That shift matters because synthetic documents are easier to insert when the control environment relies on distributed communication and asynchronous approval.

The internal control stress points are predictable. First, document intake becomes vulnerable when staff assume that a file attached to a familiar email thread must be genuine. Second, approval workflows become weak when managers sign off through remote channels that do not require identity strengthening beyond ordinary login credentials. Third, exception handling becomes fragile when the control culture rewards speed and convenience more than verification. An empirical study on e auditing adoption in Saudi Arabia found that information quality and system quality significantly affect the use of e auditing, and that stronger use is associated with

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

better internal audit department performance [27]. The implication for synthetic evidence is clear. Where document quality, metadata quality, and system quality are weak, a fabricated record can blend into the workflow more easily. Where those qualities are strong, the audit trail becomes more difficult to falsify because inconsistencies are easier to detect and investigate.

Audit procedures therefore need to evolve from passive document review to active evidence authentication. Digital bank confirmations are a useful example. Research on audit digital transformation found that digital confirmations can improve audit quality, showing that digital verification can strengthen, rather than weaken, the audit process when it is properly designed and controlled [28]. This is an important nuance. The problem is not digitization itself. The problem is digitization without adequate provenance checks, role separation, and verification discipline. A digital workflow can either increase transparency or accelerate deception depending on how authentication is embedded. For that reason, auditors should treat synthetic invoices, contracts, and approvals as control risks rather than as unusual one off anomalies.

Professional skepticism also needs to become more explicit in remote settings. In traditional audit work, a missing signature or unusual paper trail would invite follow up. In digital settings, the same logic should apply to odd language patterns, copied formatting, implausible timestamps, mismatched file histories, or suspiciously perfect attachments. The evidence base from internal audit studies suggests that procedures remain effective when auditors combine system quality, verification intensity, and human judgment rather than relying on one control layer alone.

Table 6 explains how fabricated records enter digital workflows. It highlights the control area, attack example, control failure, mitigation, and citation basis for invoice approval, remote authorization, and digital bank confirmation risks.

Table 6: Internal control vulnerabilities exposed by synthetic evidence

Control area	Attack example	Control failure	Mitigation	Citation(s)
Invoice and vendor approval	AI generated invoice or altered remittance advice	Reliance on file appearance and routine approval	Require provenance checks, maker checker review, and call back confirmation	[28]
Remote authorization	Synthetic email or chat message mimicking management approval	Weak identity assurance in digital channels	Use multifactor authentication and independent confirmation	[28]
Digital bank confirmation	Forged confirmation routed through an informal channel	Belief that digitized equals verified	Use controlled portals, audit logs, and immutable timestamps	[28]

This table outlines practical internal control weaknesses that synthetic evidence can exploit and the controls that can reduce those weaknesses. Abbreviations: AI = artificial intelligence; MFA = multifactor authentication; the table also refers to maker checker review, call back confirmation, and audit logs in full.

3.3 AI Generated Corporate Communications, Narrative Quality, and Market Perception

AI generated corporate communication is not inherently bad. In many settings, it improves grammar, consistency, speed, and readability. It can help management produce clearer drafts, maintain a more uniform tone across sections of an annual report, and reduce the delay between data collection and narrative disclosure. The difficulty is that the same tool that improves surface quality can also hollow out substance. Disclosure that sounds polished may still be shallow, selective, or strategically vague. More importantly, corporate audiences do not judge disclosure only on readability. They also judge it on authenticity, legitimacy, and intent. A recent study on AI disclosure and legitimacy found that disclosing AI use can reduce trust because it activates concerns about legitimacy and norm violation [29]. In a corporate reporting context, that means readers may interpret AI assisted narrative not merely as efficient drafting, but as a signal that the organization is distancing itself from responsibility.

This trust penalty is especially relevant when AI content is used in investor relations, sustainability reporting, and executive messaging. Another experimental study showed that AI

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

disclosure in advertisements influences trust in both the advertisement and the organization, confirming that disclosure does not simply inform audiences; it also changes how they evaluate the sender [30]. The lesson for accounting is that narrative quality is not just a stylistic issue. A report that is easy to read but difficult to trust may create a temporary communication advantage while weakening the long term credibility of the firm. Investors may become more cautious if they sense that positive language has been optimized by generative systems without sufficient managerial voice or evidential depth.

The evidence on human reactions to AI generated writing reinforces this concern. A large experimental study found a persistent AI disclosure penalty: participants consistently rated creative writing less favorably when they believed it came from AI, and the effect was mediated by perceived authenticity [31]. That finding matters because corporate storytelling often depends on exactly the same ingredients as creative writing, namely voice, tone, coherence, and the ability to make an organization appear purposeful and believable. If stakeholders infer that a firm's narrative has been heavily machine drafted, they may read it as less sincere, less accountable, and less informative even when the content is factually correct. The tension, therefore, is not between good grammar and bad grammar. It is between efficiency and authenticity, and accounting firms must recognize that both matter.

This tension is visible in market perception as well. Analysts are not only processing data. They are also interpreting tone, emphasis, and omission. A narrative that is too polished may trigger suspicion that negative facts have been softened, while a narrative that is too generic may suggest low managerial engagement. The result is a credibility problem that can affect how market participants read earnings releases, management discussion sections, and risk factor narratives.

Table 7 presents the positive effects, negative effects, evidence base, and reporting implications of AI generated communication on disclosure quality.

Table 7: AI generated communication effects on disclosure quality

Positive effects	Negative effects	Evidence base	Reporting implication	Citation(s)
Better consistency, speed, and readability	Shallow narrative depth and weaker authenticity	AI disclosure can reduce trust and credibility	Use AI for drafting, but retain clear human accountability and editing	[31]
Cleaner language and fewer typographical errors	Greater suspicion of strategic wording	AI disclosure in communication contexts alters trust judgments	Make human involvement and review procedures explicit	[31]
Faster preparation of recurring disclosures	Risk of repetitive or formulaic storytelling	Persistent AI disclosure penalty in evaluative judgments	Combine narrative efficiency with evidence rich support	[31]

This table compares the benefits and drawbacks of AI generated communication for disclosure quality. Abbreviations: AI = artificial intelligence; disclosure quality refers to consistency, readability, authenticity, narrative depth, and credibility.

3.4 Regulatory, Technical, and Assurance Countermeasures

The main lesson from recent research is that protection of digital trust cannot depend on a single fix. Content labels, provenance tools, and assurance routines each solve part of the problem, but none of them is sufficient on its own. In labeling studies, process based labels that explain how AI content was produced can reduce belief in misleading claims, while harm based labels can also shape viewers' responses, although a simple AI generated label alone may have limited effects on engagement behaviour [32]. This means that transparency needs to be designed, not merely announced. A vague disclosure that "AI was used" may satisfy a formal requirement without helping users understand whether the content is synthetic, edited, summarized, or human supervised.

That nuance matters for corporate reporting because disclosure systems should do more than warn. They should help users evaluate risk. A second experimental study found that labeling AI generated or AI enhanced content reduced both affective and behavioral engagement, especially for emotional content, while late disclosure helped only when content was AI enhanced rather than fully AI generated [33]. This suggests that transparency policies need to distinguish between content types and timing. In accounting, the equivalent would be to distinguish between AI use for spell checking, AI use for drafting, and AI

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

use for substantive narrative creation. Regulators, audit committees, and compliance teams should therefore ask not only whether AI was used, but how it was used, when it was disclosed, and who reviewed the result.

Technical provenance is the next layer. Semi automated provenance tracking in trusted research environments has been shown to improve transparency and quality assurance, while reducing data processing errors by helping teams authenticate and audit data workflows[34]. The accounting implication is straightforward. If provenance can be tracked for data linkage workflows, then similar logic should be applied to reporting workflows, document creation, and evidence transfer. Content credentials, timestamped metadata, version histories, and controlled audit logs do not eliminate deception, but they raise the cost of tampering and make post event verification more feasible. This is where audit committees, internal audit, and compliance functions become central. They should insist on policies that retain source metadata, identify AI assisted text, preserve approval trails, and escalate any material item whose origin cannot be verified.

Table 8 summarizes the regulatory response, technical tool, assurance use, limitations, and citation basis for AI labeling, provenance standards, and assurance procedures.

Table 8: Countermeasures for digital trust protection

Regulatory response	Technical tool	Assurance use	Limitations	Citation
AI content labeling rules	Process based labels and harm based warnings	Helps users interpret synthetic content	Labels alone do not guarantee behavioral change	[34]
Provenance standards	Metadata, timestamps, and content credentials	Supports source authentication and audit trails	Requires broad adoption across platforms and vendors	[34]
Assurance procedures	Verification logs and workflow tracing	Helps internal audit and compliance confirm origin	Adds cost and requires staff capability	[34]

This table presents the main countermeasures for protecting digital trust in financial reporting. Abbreviations: AI = artificial intelligence; metadata = data that describe the origin and history of a file; provenance = documented origin and transformation history.

Figure 2 presents a stepwise risk chain in which synthetic content is created, distributed, normalized, and then introduced into reporting workflows. It shows that the major failure point occurs when weak verification, detection, and editorial controls allow false content to be relied upon, leading to distortion of evidence, narrative, and trust.

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

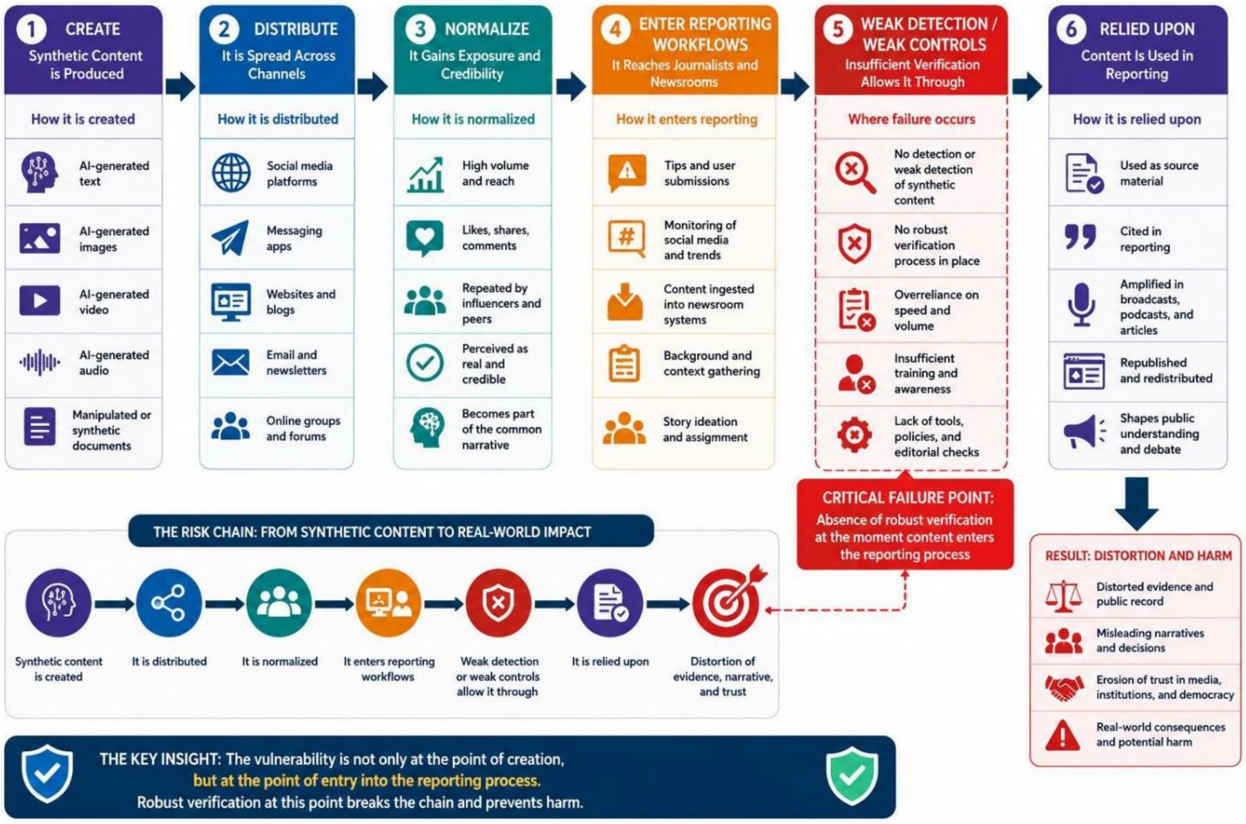

Figure 2: The Risk Chain from Synthetic Content Creation to Distortion in Reporting [32-34]

The figure maps the progression from synthetic content generation to dissemination, normalization, entry into reporting systems, and eventual reliance despite inadequate verification. Abbreviations used: AI, artificial intelligence; all other labels are written in full and require no additional abbreviation expansion.

3.5 Integrated Implications for Accounting Practice and Future Research

The integrated implication for accounting is that digital trust has become a governance issue rather than a purely technical issue. For preparers, the main challenge is to preserve authenticity while using AI to improve efficiency. For auditors, the challenge is to distinguish genuine evidence from plausible synthetic evidence without slowing the audit to an impractical pace. For regulators, the challenge is to define transparency rules that are useful rather than symbolic. For boards, the challenge is to oversee AI use without treating it as an isolated IT matter. A cross national experimental study found that transparent communication by AI companies can increase public readiness when it conveys substantial information and accountability, although the strength of those effects depends on context [35]. That finding is useful for accounting because it implies that trust is improved not by generic disclosure alone, but by disclosures that explain what was done, why it was done, and who remains accountable.

Investor dependence on AI also creates continuity risk. Early evidence from ChatGPT outages showed that trading volume declined when ChatGPT was unavailable, suggesting that investors are already relying on generative AI to support professional tasks such as processing corporate information and making trading decisions [36]. The accounting implication is that firms, analysts, and auditors now operate in an environment where AI is part of the information supply chain. When that chain is interrupted, decision quality may fall. This makes contingency planning important. Boards should ask whether the organization can continue to process disclosures, summarize evidence, and respond to inquiries if the AI tools it relies on are unavailable, compromised, or mistrusted.

The corporate disclosure literature also points to a governance condition. Research on AI disclosure in US banks found that AI disclosure is associated with financial performance only when moderated by the interaction of shareholders, the board of directors, and independent board members [37]. That

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

result is important because it shows that disclosure alone does not create value. Governance must interpret it, control it, and use it. For future research, several gaps stand out. First, detection studies still need more work on multimodal forgeries that combine voice, image, document, and text manipulation in a single event. Second, assurance research still needs stronger evidence on which verification routines are most effective in high pressure audit settings. Third, governance research should examine how audit committees actually oversee AI assisted drafting and AI aided verification. Fourth, cross country studies are needed because transparency norms, legal expectations, and trust thresholds differ across jurisdictions.

Table 9 summarizes a future agenda that is both practical and researchable. The most useful studies will probably combine experiments, archival analysis, field interviews, and system level testing, because no single method can capture the full complexity of synthetic evidence and AI mediated disclosure. The broad direction is clear: accounting must move from relying on the appearance of evidence to verifying the provenance of evidence.

Table 9: Research gaps and future agenda

Gap	Why it matters	Suggested method	Likely contribution	Citation(s)
Multimodal deepfake detection in reporting workflows	Real fraud is likely to combine audio, text, and image manipulation	Experiments plus forensic audit case studies	Better understanding of how synthetic content travels through reporting chains	[35,36]
Governance of AI assisted narrative disclosure	Boards need to know how AI changes tone, emphasis, and accountability	Archival studies and board interviews	Clearer evidence on oversight and disclosure quality	[35,37]
Assurance standards for provenance and labeling	Trust depends on whether users can verify content origin	Field studies in audit firms and regulators	Practical protocols for provenance checking and content credentials	[35,37]

This table sets out the most important research gaps and a practical agenda for future studies on digital trust in reporting. Abbreviations: AI = artificial intelligence; the table uses the terms multimodal, archival, and field studies in their ordinary research sense.

IV. CONCLUSION

This review shows that digital trust has become fundamental to credible financial reporting in an environment shaped by artificial intelligence, deepfakes, synthetic evidence, and AI generated corporate communication. The evidence indicates that AI can improve efficiency, consistency, readability, and analytical capability, but these benefits can be undermined when human accountability, verification, and governance are weak. Deepfakes and synthetic records are particularly concerning because they can imitate trusted voices, documents, images, and messages, weakening evidence reliability and creating opportunities for fraud, unauthorized decisions, and misleading disclosures. At the same time, AI assisted reporting can produce polished narratives while raising concerns about authenticity, transparency, and managerial responsibility. The review therefore concludes that protecting digital trust requires more than sophisticated technology. Organizations need integrated controls that combine provenance tracking, secure authentication, transparent AI use, independent verification, strong approval procedures, skepticism, and board oversight. Regulators and professional bodies should establish clear principles for AI disclosure and evidence verification that reflect information materiality and risk. Firms should also retain human responsibility for reporting judgments and maintain reliable audit trails for digitally generated or modified content. Future research should move beyond conceptual discussion toward empirical testing of practical solutions. Particular attention should be given to multimodal deepfakes, synthetic audit evidence, AI assisted narrative disclosures, provenance standards, and verification controls under realistic conditions. Cross national studies should examine how regulation, governance, and stakeholder expectations shape digital trust. Ultimately, trustworthy financial reporting will depend on ensuring that technological innovation strengthens, rather than replaces, accountability, evidence quality, and judgment.

ACKNOWLEDGEMENT

The authors sincerely acknowledge the researchers and scholarly communities whose published work provided the evidence and perspectives synthesized in this comprehensive

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

review. We also appreciate the academic support and intellectual contributions that helped shape the development of this manuscript.

CONFLICTS OF INTEREST

The authors declare that there are no financial, professional, or personal conflicts of interest that could have influenced the preparation or conclusions of this manuscript. All authors contributed to the work objectively and independently.

REFERENCES

[1] Li J. Artificial intelligence innovation and financial report quality. *International Review of Economics & Finance*. 2026;105:104832. https://doi.org/10.1016/j.iref.2025.104832

[2] Alruwaili TF, Mgammal MH. The impact of artificial intelligence on accounting practices: an academic perspective. *Humanities and Social Sciences Communications*. 2025;12:1197. https://doi.org/10.1057/s41599-025-05004-6

[3] Küster S, Steindl T, Göttsche M. The informational content of key audit matters: evidence from using artificial intelligence in textual analysis. *Contemporary Accounting Research*. 2025;42(4):2392-2423. https://doi.org/10.1111/1911-3846.13070

[4] Elsayed N. Strategic AI disclosures and legitimacy: impression management in UK FTSE100 annual reports. *International Journal of Accounting Information Systems*. 2025;56:100757. https://doi.org/10.1016/j.accinf.2025.100757

[5] Murikah W, Nthenge JK, Musyoka FM. Bias and ethics of AI systems applied in auditing: a systematic review. *Scientific African*. 2024;25:e02281. https://doi.org/10.1016/j.sciaf.2024.e02281

[6] Romero-Moreno F. Deepfake detection in generative AI: a legal framework proposal to protect human rights. *Computer Law & Security Review*. 2025;58:106162. https://doi.org/10.1016/j.clsr.2025.106162

[7] Lombardi DR, Kim M, Sipior JC, Vasarhelyi MA. The increased role of advanced technology and automation in audit: a Delphi study. *International Journal of Accounting Information Systems*. 2025;56:100733. https://doi.org/10.1016/j.accinf.2025.100733

[8] Laine J, Minkkinen M, Mäntymäki M. Ethics-based AI auditing: a systematic literature review on conceptualizations of ethical principles and knowledge contributions to stakeholders. *Information & Management*. 2024;61(5):103969. https://doi.org/10.1016/j.im.2024.103969

[9] Bin-Nashwan SA, Li JZ, Jiang H, Bajary AR, Ma'aji MM. Does AI adoption redefine financial reporting accuracy, auditing efficiency, and information asymmetry? An integrated model of TOE-TAM-RDT and big data governance. *Computers in Human Behavior Reports*. 2025;17:100572. https://doi.org/10.1016/j.chbr.2024.100572

[10] Alhazmi AHJ, Islam SMN, Prokofieva M. The impact of artificial intelligence adoption on the quality of financial reports on the Saudi Stock Exchange. *International Journal of Financial Studies*. 2025;13(1):21. https://doi.org/10.3390/ijfs13010021

[11] Oesterreich TD, Anton E, Hettler FM, Teuteberg F. What drives individuals' trusting intention in digital platforms? An exploratory meta-analysis. *Management Review Quarterly*. 2025;75:3615-3667. https://doi.org/10.1007/s11301-024-00477-2

[12] Glassberg I, Brender Ilan Y, Zwilling M. The key role of design and transparency in enhancing trust in AI-powered digital agents. *Journal of Innovation & Knowledge*. 2025;10:100770. https://doi.org/10.1016/j.jik.2025.100770

[13] Vancisin T, Clarke L, Orr M, Hinrichs U. Provenance visualization: tracing people, processes, and practices through a data-driven approach to provenance. *Digital Scholarship in the Humanities*. 2023;38(3):1322-1339. https://doi.org/10.1093/llc/fqad020

[14] Alanazi S, Asif S. Exploring deepfake technology: creation, consequences and countermeasures. *Human-Intelligent Systems Integration*. 2024;6:49-60. https://doi.org/10.1007/s42454-024-00054-8

[15] Momin MD, Sufian A, Barman D, Leo M, Distante C, Damer N. Explainable deepfake detection across different modalities: an overview of methods and challenges. *Image and Vision Computing*. 2025;163:105738. https://doi.org/10.1016/j.imavis.2025.105738

[16] Alali A, Theodorakopoulos G. Partial fake speech attacks in the real world using deepfake audio. *Journal of Cybersecurity and Privacy*. 2025;5(1):6. https://doi.org/10.3390/jcp5010006

[17] Hossain A, Bose S, Shamsuddin A. Do integrated report readability and tone convey value relevant information? International evidence. *Journal of Contemporary Accounting & Economics*. 2025;21(3):100488. https://doi.org/10.1016/j.jcae.2025.100488

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

[18] Sahebi S, Formosa P, Bankins S. The AI penalty and disclosure paradox: trust, authenticity and knowledge uptake in AI-mediated communication. *Computers in Human Behavior: Artificial Humans*. 2026;8:100304. https://doi.org/10.1016/j.chbah.2026.100304

[19] Ciccola R, Guidi M, Chiucchi MS, Giuliani M. Artificial intelligence and sustainability reporting in practice: projections from an intellectual capital perspective. *VINE Journal of Information and Knowledge Management Systems*. 2025:1-23. https://doi.org/10.1108/VJIKMS-08-2025-0360

[20] Akter M, Kummer TF, Yigitbasioglu O. Looking beyond the hype: the challenges of blockchain adoption in accounting. *International Journal of Accounting Information Systems.* 2024;53:100681. https://doi.org/10.1016/j.accinf.2024.100681

[21] Bossler LF, Buchwald A, Spohrer K. And no one gets the short end of the stick: a blockchain-based approach to solving the two-sided opportunism problem in interorganizational information sharing. *Information Systems Research.* 2025;36(3):1565-1586. https://doi.org/10.1287/isre.2022.0065

[22] Große N, Möller F, Schoormann T, Henke M. Designing trust-enabling blockchain systems for the inter-organizational exchange of capacity. *Decision Support Systems*. 2024;179:114182. https://doi.org/10.1016/j.dss.2024.114182

[23] Malinka K, Firc A, Šalko M, Prudký D, Radačovská K, Hanáček P. Comprehensive multiparametric analysis of human deepfake speech recognition. *EURASIP Journal on Image and Video Processing*. 2024;2024:24. https://doi.org/10.1186/s13640-024-00641-4

[24] Lavan N, Irvine M, Rosi V, McGettigan C. Voice clones sound realistic but not (yet) hyperrealistic. *PLoS One.* 2025;20(9):e0332692. https://doi.org/10.1371/journal.pone.0332692

[25] Pham L, Lam P, Tran D, Tang H, Nguyen T, Schindler A, et al. A comprehensive survey with critical analysis for deepfake speech detection. *Computer Science Review*. 2025;57:100757. https://doi.org/10.1016/j.cosrev.2025.100757

[26] Jarva H, Zeitler T. Implications of the COVID-19 pandemic on internal auditing: a field study. *Journal of Applied Accounting Research.* 2024;25(2):355-370. https://doi.org/10.1108/JAAR-12-2021-0333

[27] Mujalli A. The influence of E-auditing adoption on internal audit department performance amid COVID-19 in Saudi Arabia. *Cogent Business & Management.* 2024;11(1):2295608. https://doi.org/10.1080/23311975.2023.2295608

[28] Guo R, Jia Y, Shentu L. The effect of audit digital transformation on audit quality: evidence from digital bank confirmations. *China Journal of Accounting Studies.* 2025;13(3):247-281. https://doi.org/10.1080/21697213.2024.2442769

[29] Schilke O, Reimann M. How does AI disclosure shape trust? Unpacking the role of legitimacy. *Social Psychology Quarterly*. 2026. https://doi.org/10.1177/01902725261425997

[30] Koning B, Voorveld HAM. Disclaimer! This content is AI-generated: how AI disclosures influence trust in advertisements and organizations. *Journal of Interactive Advertising*. 2025;25(3):240-253. https://doi.org/10.1080/15252019.2025.2554149

[31] Raj M, Berg JM, Seamans R. The artificial intelligence disclosure penalty: humans persistently devalue AI-generated creative writing. *Journal of Experimental Psychology: General*. 2026;155(4):896-915. https://doi.org/10.1037/xge0001889

[32] Wittenberg C, Epstein Z, Péloquin-Skulski G, Berinsky AJ, Rand DG. Labeling AI-generated media online. *PNAS Nexus.* 2025;4(6):pgaf170. https://doi.org/10.1093/pnasnexus/pgaf170

[33] Seeger F, Wessel M, Lehrer C. AI content labeling and user engagement on social media: the role of AI level, content type, and disclosure timing. *Electronic Markets*. 2026;36:31. https://doi.org/10.1007/s12525-026-00883-2

[34] O'Sullivan K, Markovic M, Dymiter J, Scheliga B, Odo C, Wilde K. Semi-automated data provenance tracking for transparent data production and linkage to enhance auditing and quality assurance in Trusted Research Environments. *International Journal of Population Data Science*. 2025;10(2):2464. https://doi.org/10.23889/ijpds.v10i2.2464

[35] Xu H, Dong C. The responsibility to inform: how AI companies' transparent communication practice influences public readiness in a cross-national context. *Communication and Change*. 2026;2:4. https://doi.org/10.1007/s44382-026-00024-5

[36] Cheng Q, Lin P, Zhao Y. Does generative AI facilitate investor trading? Early evidence from ChatGPT outages. *Journal of Accounting and Economics*. 2025;80(2-3):101821. https://doi.org/10.1016/j.jacceco.2025.101821

[37] Alzeghoul A, Alsharari NM. Impact of AI disclosure on the financial reporting and performance as evidence from

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 8, pp 77-93, August-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.308008
Available Online at https://www.jaiet.com

US banks. *Journal of Risk and Financial Management.* 2025;18(1):4. https://doi.org/10.3390/jrfm18010004

Citation of this Article:

Boluwatife Gabriel Jesutoye, Sodeeq Ipadeola Olalekan, David Chinonso Anih, Ahmed Oladapo Olaneye & Oyewole Abdulateef Ojora. (2026). Digital Trust in Financial Reporting: A Review of Deepfakes, Synthetic Evidence, and AI Generated Corporate Communications. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 3(8), 77-93. Article DOI: https://doi.org/10.47001/JAIET/2026.308008

***** End of the Article *****