International Journal of Science, Strategic Management and Technology
Volume **02** Issue **11** November-2026 | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Data Governance and Ethical Issues in Accounting Technology

CMA Venkata Ramesh Tumu – FCMA, LLB, CFE, CRISC, Practicing Cost Accountant and Virtual CFO, Pursuing PhD at KLU

Neelam Padmalatha – M.Com, Assistant Professor, Bhavan's Vivekananda College of Commerce with 32 years of experience

https://doi.org/10.55041/ijsmt.v2i11.017

Cite this Article: Tumu, C. V. R. & Padmalatha, N. (2026). Data Governance and Ethical Issues in Accounting Technology. International Journal of Science, Strategic Management and Technology, *02*(11), 1-9. https://doi.org/10.55041/ijsmt.v2i11.017

License: This article is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting use, distribution, and reproduction in any medium, provided the original author(s) and source are properly credited.

Abstract

Purpose: The introduction of advanced technologies like artificial intelligence (AI), blockchain, and enterprise resource planning (ERP) systems has transformed accounting practices, allowing for quicker processing, greater transparency, and more informed decision-making. Despite these benefits, they also bring up crucial concerns related to data governance and ethical responsibility. This paper explores how governance frameworks and ethical standards can be applied to ensure trust, adherence to regulations, and integrity in technology-driven accounting settings.

Methodology: This study utilizes a conceptual and case-based approach, referencing regulatory frameworks such as IFRS, Indian Accounting Standards (Ind AS), GDPR, and the EU AI Act. It addresses ethical challenges like bias in AI predictions, transparency in disclosures, risks of fraud in digital records, and responsibility for technology-driven mistakes. Case studies, including ERP breaches revealing client information, incorrect reporting of crypto assets due to a lack of standards, and inaccuracies in ESG reporting, are analyzed to demonstrate real-world issues.

Findings: The research finds that strong data governance ensures accuracy, integrity, and compliance, while ethical oversight protects stakeholder trust. Weak governance leaves organizations vulnerable to cybersecurity threats, harm to reputation, and regulatory fines. Excessive reliance on automation without professional skepticism weakens ethical judgment, while emerging areas such as ESG reporting and blockchain require new accountability frameworks. **The findings highlight that accountants must transition from traditional record keepers to digital stewards of trust.**

Implications: The paper suggests practical strategies, **including forming AI governance councils,** performing regular audits for bias and security, and incorporating ESG metrics into accounting systems. It advocates for a **balanced approach** where innovation aligns with compliance and ethics, ensuring that technology bolsters rather than compromises financial integrity. By **embedding governance and ethical principles** into accounting technology, organizations can enhance stakeholder trust and create resilient financial systems.

Keywords: Data Governance, Accounting Technology, Ethical Issues, Artificial Intelligence, Blockchain, ERP Systems, ESG Reporting, Compliance, Cybersecurity, Financial Integrity

1. Introduction

The accounting profession is undergoing an unprecedented digital transformation. Historical manual ledgers and static spreadsheet systems have given way to integrated Enterprise Resource Planning (ERP) platforms, decentralized blockchain ledgers, automated algorithmic workflows, and predictive Artificial Intelligence (AI) analytics. These technological advancements have revolutionized financial engineering, accelerating processing speeds, improving data accuracy, and enabling real-time financial reporting. However, the rapid

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

integration of accounting technology introduces significant data governance and ethical vulnerabilities. Financial environments now generate, process, and store vast volumes of sensitive quantitative and qualitative data across complex, interconnected networks. Without robust data governance protocols, organizations face elevated risks of cybersecurity breaches, algorithmic biases, regulatory non-compliance, and data manipulation. Moreover, the automated nature of modern financial systems risks encouraging over-reliance on technology, potentially dulling the professional scepticism required for sound auditing and financial reporting. To address these challenges, accounting governance must evolve beyond traditional internal controls to encompass holistic data privacy, algorithmic accountability, and technical compliance. This research analyses how theoretical data governance frameworks and ethical standards can be operationalized within contemporary financial infrastructure. By synthesizing multi-jurisdictional regulatory frameworks—including IFRS, Ind AS, GDPR, and the EU AI Act—and examining real-world empirical case studies, this study outlines a strategic roadmap for maintaining financial integrity in the digital age.

2. Theoretical Framework & Conceptual Foundations

2.1 Theoretical Framework

This study is grounded in three core theoretical Theories:

1. **Agency Theory:** In technology-mediated accounting, agency conflicts extend beyond managers and shareholders to include algorithmic systems ("algorithmic agents"). When AI systems optimize financial parameters without human oversight, principal-agent information asymmetries can widen, leading to unverified or biased financial reporting.

2. Technology Acceptance Model (TAM) & Technological Determinism: While TAM emphasizes perceived usefulness and ease of use in technology adoption, uncritical acceptance can foster ‘automation bias’. Finance professionals may accept automated outputs without questioning the underlying assumptions or dataset integrity

3. Stakeholder Theory & Legitimacy Theory: Organizations depend on broad stakeholder trust. Unethical data handling, opaque AI models, or inaccurate ESG metrics jeopardize organizational legitimacy and stakeholder value

2.2 Core Dimensions of Accounting Technology Data Governance

Data governance in accounting involves the structural alignment of policy, architecture, and accountability. It spans five key operational pillars:

Pillar	**Focus**	**Strategic Risk / Vulnerability**
Data Quality & Lineage	Verifying original data sources and processing steps	Unrecognized pipeline corruption leading to invalid reports
Data Privacy & Protection	Safeguarding employee, client, and vendor PII	High regulatory penalties under GDPR/DPDP laws
Algorithmic Accountability	Auditing decision mechanisms within AI/ML models	"Black-box" opacity obscuring model error or bias
System Interoperability	Maintaining structural integrity across ERP/cloud systems	Unsynchronized data siloing creating report discrepancies
Cyber Resiliency	Protecting financial systems against breaches	System outage, ransomware loss, and unauthorized access

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

3. Regulatory Alignment Dynamics: Global & Regional Perspectives

The intersection of accounting systems and data architecture is governed by an evolving regulatory matrix spanning accounting standards, data privacy mandates, and AI regulations.

3.1 Accounting Standards: IFRS and Ind AS

IFRS 9 / Ind AS 109 (Financial Instruments): Mandates Expected Credit Loss (ECL) provisioning based on forward-looking macroeconomic data. Automated ECL models heavily rely on machine learning algorithms. If training datasets contain historical bias or fail to reflect structural economic shifts, calculated loan-loss provisions become fundamentally flawed.

IFRS 13 / Ind AS 113 (Fair Value Measurement): Establishes valuation hierarchies (Levels 1, 2, and 3). Valuing complex digital assets, smart contracts, and unlisted tech securities under Level 3 inputs requires algorithmic models whose valuation parameters must remain fully transparent and verifiable.

IAS 38 / Ind AS 38 (Intangible Assets): Defines criteria for recognizing intangible assets, directly affecting how internally generated software, databases, and proprietary AI algorithms are capitalized versus expensed.

3.2 Privacy and Algorithmic Regulation:GDPR and the EU AI Act

General Data Protection Regulation (GDPR): Enforces strict limits on processing Personally Identifiable Information (PII). Article 5 requires data minimization and purpose limitation, while Article 22 grants individuals rights against purely automated decision-making. Accounting systems that process payroll, vendor master files, and consumer credit data must embed *Privacy by Design*.

EU AI Act: Formally classifies AI technologies used in critical infrastructure, credit scoring, and financial risk evaluation as high-risk systems. Organizations must establish risk management protocols, maintain detailed technical documentation, ensure human oversight, and audit training datasets for bias

4. Methodology & Comparative Case Analysis

This research looks at real-world problems in three important areas: how companies operate, their digital assets, and how they report on sustainability. It uses a qualitative approach, studying multiple cases to understand the issues.

4.1 Case A: Enterprise ERP Data Breach and Internal Control Collapse

Context:A multinational logistics provider experienced an unauthorized breach of its cloud-hosted ERP system due to misconfigured access permissions and unpatched API endpoints.

Impact: More than 450,000 confidential records were made public, including bank account information, tax IDs, and sensitive client pricing data. This breach had a major impact on the company's financial operations, causing delays in their financial reporting and attracting the attention of regulators, who launched investigations under the General Data Protection Regulation (GDPR). As a result, the company's reputation suffered significantly.

Root Cause Analysis: Insufficient data segregation, inadequate multi-factor authentication for administrative accounts, and lack of continuous log monitoring.

4.2 Case B: Misreporting and Valuation Failures in Digital Crypto-Assets

Context: A fintech conglomerate accumulated substantial holdings in decentralized digital tokens and utility crypto-assets.

Impact: Due to the absence of clear GAAP/IFRS directives tailored to volatile crypto-assets, the enterprise misclassified non-liquid tokens as liquid cash equivalents under IAS 2/IAS 38 rather than applying fair-value impairment models. When market liquidity contracted, the company recorded an unannounced $180 million write-down, triggering shareholder litigation and regulatory enforcement.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Root Cause Analysis: Opaque automated valuation feeds (oracle price feeds) without manual override protocols, combined with non-standardized accounting treatment across international subsidiaries.

4.3 Case C: Automated ESG Metrics Discrepancies and Greenwashing

Context: A global energy provider utilized an automated software suite to track Scope 1, Scope 2, and Scope 3 carbon emissions across its operational facilities.

Impact: The company's software had a big mistake in how it calculated carbon emissions from its factories overseas. This mistake made it seem like the company was producing 34% less carbon emissions than it actually was. The company used these wrong numbers to tell investors and the public about its environmental impact. It even sold special bonds that were supposed to be good for the environment. But when outside auditors found the mistake, the company got in trouble for making false claims about being environmentally friendly. It also had to deal with problems related to its bonds and faced penalties from the government. This was a big issue because it made people question whether the company was really committed to reducing its environmental impact or just trying to look good.

Root Cause Analysis: Blind reliance on third-party vendor algorithms without independent data verification or internal audit oversight.

5. Findings & Ethical Dimensions in Modern Accounting

Synthesizing case evidence and theoretical models reveals four major ethical vulnerabilities in modern accounting technology:

5.1 Algorithmic Bias and Discriminatory Financial Analytics

Automated credit scoring and underwriting algorithms often reflect historical societal biases embedded within their training data. In automated accounts receivable management, predictive collection algorithms may systematically assign higher credit risk scores to businesses in specific geographic or demographic categories, perpetuating systemic economic inequality.

5.2 Opacity and the "Black-Box" Problem

As deep neural networks and complex machine learning models handle financial forecasting, credit provisioning, and audit sampling, the underlying logic of these models becomes opaque—even to the system developers. This "black-box" nature conflicts with fundamental accounting standards requiring verifiable, reproducible, and explainable financial statements.

5.3 Degradation of Professional Skepticism (Automation Bias)

Excessive reliance on automated ERP systems and AI tools risks creating a passive compliance mindset. Accountants and auditors may accept automated system outputs without verifying source documentation or challenging underlying assumptions. This degradation of professional skepticism weakens the critical defensive barrier against financial misstatements and fraud.

5.4 Fraud Transformation: Digital Ledgers and Smart Contracts

While blockchain ledgers provide immutable transaction logs, they do not guarantee the underlying accuracy or legitimacy of input data. Fraudulent or incorrect data entered onto a blockchain becomes permanently recorded, creating a permanent, erroneous record. Similarly, vulnerabilities in automated smart contract code can be exploited to transfer funds improperly, leaving automated systems with limited capacity for immediate corrective intervention.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

6. Strategic Implications & Recommendations: The Digital Steward Framework

To bridge the gap between technological innovation and financial integrity, organizations must implement a multi-layered Governance Framework. Accountants must expand their traditional roles, transitioning into proactive digital stewards of trust.

6.1 Actionable Implementation Matrix

Governance Dimension	Strategic Action	Operational Mechanism	Expected Outcome
Enterprise Governance	Establish AI Governance Councils	Cross-functional board comprising CFO, CISO, Chief Data Officer, and Legal Counsel	Strategic alignment between tech deployment and regulatory mandates.
Model Verification	Continuous Algorithmic Auditing	Periodic third-party model audits, bias stress-testing, and drift analysis	Early detection of algorithmic drift, bias, and calculation errors.
Data Security	Zero-Trust Architecture	Role-based access control (RBAC), end-to-end encryption, multi-factor authentication	Elimination of unauthorized data access and reduced risk of ERP breaches.
ESG Oversight	Integrated ESG Controls	Standardized data intake pipelines with automated and manual verification checkpoints	Accurate, verifiable, and audit-ready sustainability disclosures.
Human Competency	Professional Reskilling	Professional development combining forensic accounting, data ethics, and AI analytics	Preservation of professional skepticism and enhanced digital risk management.

6.2 Key Operational Initiatives

1. AI Governance Councils: Establish specialized governing bodies tasked with approving algorithm models, evaluating dataset representativeness, and establishing accountability protocols before deploying financial AI applications.

2. Continuous Algorithmic Auditing: Implement automated audit routines to continuously monitor system logs, verify data inputs, detect model drift, and evaluate algorithmic fairness in real time.

3. **Human-in-the-Loop" Controls:**Require mandatory manual review and sign-off by qualified accounting professionals for high-risk automated outputs, such as material asset valuations, major credit decisions, and significant accrual estimates.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

7. Conclusion & Future Research Directions

The integration of AI, blockchain, and enterprise resource planning systems has fundamentally transformed accounting practices. While these technologies deliver notable gains in processing speed and operational efficiency, they also introduce complex risks surrounding data governance, privacy compliance, algorithmic bias, and operational integrity.

Financial integrity in the digital era requires more than technical compliance; it demands robust data governance frameworks, continuous algorithmic auditing, and an unyielding commitment to professional skepticism. By embracing their expanding role as digital stewards of trust, accounting professionals can ensure that technology enhances—rather than undermines—financial reporting integrity and stakeholder confidence.

Future Research Directions

Future empirical research should focus on:

1. Developing quantitative frameworks to measure algorithmic risk within AI-driven financial reporting systems.

2. Assessing the auditability of complex decentralized finance (DeFi) protocols and multi-chain blockchain ledgers.

3. Evaluating the operational impact of emerging regional AI regulations on corporate compliance costs and reporting quality across jurisdictions.

References

- Al-Sartawi, A. M. A. M. (2020). Information technology and the accounting profession: A review and synthesis of the literature. *Journal of Financial Reporting and Accounting,* 18(2), 321–342.
- Arnaboldi, M., Busco, C., & Cuganesan, S. (2017). Accounting and performance measurement in the digital era: Large-scale possibilities and challenges. *Accounting, Auditing & Accountability Journal*, 30(4), 762–768.
- European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation - GDPR). *Official Journal of the European Union*.
- International Accounting Standards Board (IASB). (2023). *IFRS Accounting Standards: Required Annotated IFRS Standards*. IFRS Foundation.
- Ministry of Law and Justice, Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*. The Gazette of India.
- Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting*, 14(1), 115–122.
- Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big Data in accounting: An overview. *Accounting Horizons*, 29(2), 381–396.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.