Page 904 - 915 **DOI:** *https://doij.org/10.10000/IJLMH.119765*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

© 2025 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for "free" and "open access" by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Beyond the Balance Sheet: Cyber Law & Forensic Audit through the NFRA Lens

KHUSH DALBIR[1] AND DHAWAL SHANKAR SRIVASTAVA[2]

ABSTRACT

Digital accounting fraud increasingly exploits code centric vulnerabilities—ledger tampering, bot generated invoices, deep fake documentation and ransomware—to outpace conventional audit defences. This article examines how India's National Financial Reporting Authority (NFRA) can integrate forensic audit analytics with cyber law enforcement to address this threat. Employing doctrinal and comparative analysis, it (i) traces the technological vectors that enable financial statement manipulation; (ii) evaluates the statutory framework under the Companies Act 2013, the amended Information Technology Act 2000 and NFRA Rules 2018; (iii) reviews pivotal Indian and foreign case law; and (iv) benchmarks India's approach against the U.S. Sarbanes Oxley model, EU Audit Regulation 537/2014 and United Nations Convention against Corruption (UNCAC) mandates. The study identifies key enforcement gaps—data localisation frictions, limited cyber forensic capacity and procedural delays—and proposes a reform agenda that includes key escrow legislation, AI driven anomaly detection, mandatory Cyber Controls Assurance Reports and fast track e fraud benches. By advocating a convergence regime that couples continuous controls monitoring with cross border evidence protocols, the paper offers a blueprint for bolstering audit reliability and investor confidence in India's aspirational US$ 5 trillion digital economy.

I. INTRODUCTION

The fourth industrial revolution has ushered in an era of hyper-connected, data-driven corporate ecosystems. Contemporary accounting platforms harness artificial intelligence (AI), cloud-native enterprise-resource-planning (ERP) suites, robotic process automation, and application-programming-interface (API) gateways to process transactions at petabyte scale and near-real-time velocity. These technological affordances augment efficiency, yet they concomitantly multiply the number of attack vectors that sophisticated actors can exploit. *Digital accounting fraud*—broadly defined as any intentional misrepresentation or manipulation of electronically stored or transmitted financial information—has therefore

[1] Author is a LL.M (Cyber Law) Student at IILM University, Greater Noida, India.
[2] Author is an Assistant Professor at School of Law, IILM University, Greater Noida, India.

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

become one of the most pernicious threats to audit reliability, investor confidence, and macro-economic stability.

In the Indian regulatory constellation, the National Financial Reporting Authority (NFRA) is statutorily tasked, under section 132 of the *Companies Act 2013*, with prescribing auditing standards, inspecting statutory auditors, and investigating professional misconduct. As digital-first fraud tactics proliferate—from SQL-injection assaults on general-ledger databases to machine-generated invoice spam that inflates revenue—NFRA must increasingly knit together forensic audit disciplines with India's evolving cyber-law apparatus. This article probes how such an integrated enforcement paradigm can detect, investigate, and deter digital accounting fraud. It adopts a comparative jurisprudential lens, drawing insights from the United States' *Sarbanes-Oxley Act 2002*, the European Union's *Audit Regulation 537/2014* and *General Data Protection Regulation (GDPR) 2016*, as well as UNCAC frameworks.

II. CONCEPTUAL UNDERSTANDING

Definitional contours

Digital accounting fraud occupies the intersection of corporate malfeasance and cybercrime. It now manifests in an ever-widening taxonomy that includes, but is not limited to:

Ledger tampering – unauthorised alteration of database entries within an ERP system, often by editing SQL tables after period close and back-dating the transaction timestamp to evade routine reconciliations.

Automated invoice farms – bot-driven generation of thousands of fictitious B2B invoices that temporarily inflate receivables and turnover ratios, enabling management to hit performance covenants and trigger bonus payouts.

Deep-fake audit trails – deployment of generative-AI models to fabricate PDF vendor contracts, e-mail confirmations, and even video conference clips, thereby creating the illusion of underlying economic activity where none exists.

Privilege-escalation misuse – insiders who possess—or gain—administrator rights override change-logging controls to modify journal vouchers post-close, then purge the audit trail using log-scrubbing scripts.

Ransomware blackmail – encryption of accounting archives followed by extortion, frequently coupled with threats to leak evidence of pre-existing fraud unless hush-money is paid.

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

Shadow-IT spreadsheets – off-ledger Excel or Google-Sheet models maintained by a single employee or desk that feed manual topside adjustments into the general ledger without independent review, masking losses or inflating asset valuations.

API-token hijacking – compromise of payment-gateway or GST e-invoice API keys, allowing attackers to issue phoney credit-notes or manipulate tax ledgers, thereby distorting net revenue and input-tax-credit figures.

Cloud-misconfiguration diversion – exploiting weak Identity and Access Management (IAM) policies on cloud-hosted ERP instances to clone production databases to attacker-controlled accounts, where records are altered before being re-injected, effectively laundering the audit trail.

Synthetic-identity payroll – creation of ghost employees using AI-generated KYC documents; salaries are routed to mule accounts, inflating personnel expenses and facilitating misappropriation of cash.

IoT-sensor spoofing in inventory systems – tampering with RFID or weight-sensor data feeds to overstate warehouse stock levels, leading to false cost-of-sales calculations and overstated gross margins.

Smart-contract manipulation – in blockchain-enabled supply chains, malicious alteration of oracles or contract logic to mis-state asset transfers or receivables, making on-chain audit trails appear legitimate when underlying economic reality is counterfeit.

AI-assisted round-tripping – algorithmic routing of the same funds through nested shell companies and returning them as purported revenue, with machine-generated supporting documentation that passes keyword-based compliance checks.

Distinguishing characteristics

Traditional audit failures—typified by manual understatement of liabilities—leave paper trails amenable to sample-based vouching. Digital fraud, by contrast, leverages *speed*, *scale*, and *stealth*. Logs can be programmatically purged; transactions routed through anonymising proxies; and evidence stored on offshore cloud nodes outside Indian jurisdiction. Detection therefore demands (i) continuous-controls monitoring, (ii) data-forensic imaging, (iii) blockchain for immutability, and (iv) strong cyber-law provisions on cross-border data access.

Synergy between cyber law and forensic audit

Forensic auditors deploy specialised scripts (e.g., Benford's-Law analyzers) to surface

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

anomalies, but admissibility hinges on the *Information Technology Act 2000* (IT Act) and the *Indian Evidence Act 1872* (as amended 2023) permitting hash-authenticated electronic records. Cyber law thus furnishes the evidentiary scaffolding, while forensic audit provides the investigative horsepower—each incomplete without the other.

III. HISTORICAL AND LEGISLATIVE BACKGROUND

Global evolution

The Enron collapse (2001) catalysed the US Congress to enact the *Sarbanes-Oxley Act* (SOX), embedding Public Company Accounting Oversight Board (PCAOB) inspections and CEO/CFO certification mandates. Parallelly, the EU's 8th Directive (2006) sought to harmonise statutory-audit oversight. By 2015, cyber-enabled frauds such as Tesco Bank's £2.26 million breach and Wirecard's €1.9 billion accounting hole highlighted how network intrusions could camouflage financial fakery.

Indian inflection points

Satyam Computer Services Ltd (2009): One of India's most infamous corporate frauds, the Satyam scandal involved the fabrication of ₹7,136 crore in revenues through fictitious fixed deposit (FD) receipts and inflated cash balances. This case exposed deep flaws in auditor independence and oversight, triggering regulatory calls for an autonomous audit supervisory body. It laid the groundwork for the eventual formation of NFRA under the Companies Act 2013.

IL&FS Group (2018): The collapse of IL&FS revealed the misuse of complex Special Purpose Vehicle (SPV) structures and manipulation of loan provisioning to conceal mounting solvency issues. The investigation relied heavily on forensic audits conducted by the SFIO and Grant Thornton, which used SQL dump analyses and metadata-tracked email correspondence to uncover the scale of financial misrepresentation. The importance of cyber-forensics in modern financial investigations has been highlighted by this case.

Legislative Milestones

Information Technology Act 2000 (as amended 2008): This Act established India's cyberlaw framework, introducing Sections 43A, 65, and 66, which criminalise unauthorised access, hacking, identity theft, and manipulation of computer source code. These provisions support the use of digital forensics in financial fraud enforcement.

Companies Act 2013, Sections 447–452: The Companies Act 2013 substantially intensifies the legal repercussions for corporate fraud. Section 447 provides a broad definition of fraud and

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

empowers NFRA and other authorities to investigate misconduct using both documentary and electronic evidence. These provisions also enable criminal prosecution.

NFRA Rules 2018: These rules bring NFRA's regulatory architecture into operation, detailing its powers for inspection, disciplinary review, and requisition of electronic audit records. The framework has enabled NFRA to systematically incorporate cyber-forensic practices in its oversight of statutory audits.

IV. STATUTORY FRAMEWORK AND LEGAL PROVISIONS

India

Companies Act 2013

Section 447 of the Companies Act provides a sweeping definition of fraud, covering any act, omission, concealment, or abuse of position intended to deceive, gain undue advantage, or cause injury. This wide framing ensures that both traditional and digital accounting frauds fall within its ambit. Section 132 grants NFRA the authority to investigate auditors and impose penalties up to ten times the audit fee. Rule 8 of the NFRA Rules 2018 empowers NFRA to requisition "any electronic record" from auditors or auditees, a crucial provision for accessing digital ledgers and metadata.

IT Act 2000

The Information Technology Act criminalises several cyber offences that are instrumental in digital accounting fraud. Section 65 penalises the tampering of computer source code, while Section 66C targets identity theft involving digital credentials. When sensitive personal data is disclosed in breach of lawful contracts, section 72A mandates compensation. These provisions are particularly vital in scenarios involving unauthorised system access, insider leaks, or manipulation of audit software and e-records.

Evidence Act 1872 (replaced by Bharatiya Sakshaya Adhiniyam, 2023)

Section 65B outlines the procedure for admissibility of electronic records in court, requiring a certificate authenticating the origin and integrity of the evidence. In *Arjun Panditrao Khotkar v. Kailash Kushanrao* (2020), the Supreme Court clarified that server logs, hash values, and disk images can be valid evidence when accompanied by a proper 65B certificate. This clarification is pivotal for validating forensic evidence collected from ERP systems, emails, and encrypted databases in fraud cases.

Foreign jurisdictions

In the **United States**, the *Sarbanes-Oxley Act 2002* governs digital accounting fraud with key provisions such as Section 404, which mandates internal controls attestation by management and auditors, and Section 802, that criminalises the destruction of electronic records. These provisions are enforced primarily by the **Public Company Accounting Oversight Board (PCAOB)** and the **Securities and Exchange Commission (SEC)**.

In the **European Union**, the legal framework includes the *Audit Regulation 537/2014* and the *General Data Protection Regulation (GDPR) 2016*. Notably, the regulation enforces mandatory audit rotation for statutory auditors, while Article 32 of the GDPR requires security of data processing, which is directly relevant in the context of protecting financial data from cyber intrusions. Oversight is provided by the **European Securities and Markets Authority (ESMA)** and **National Competent Authorities (NCAs)** within member states.

In the **United Kingdom**, the *Fraud Act 2006* defines the offence of false representation as a central provision applicable to digital fraud, while the *UK SOX consultation (2022)* proposed a statutory requirement for directors to publish internal controls statements. However, the government opted for a Code-based approach instead of a legislative one, inviting the **Financial Reporting Council** (FRC) to strengthen the UK Corporate Governance Code. This Code-based approach includes provisions for directors to make annual declarations on the effectiveness of their company's internal controls. Enforcement is overseen by the **FRC**, which is responsible for audit regulation, corporate governance, and financial reporting integrity.

V. CASE LAW ANALYSIS

India

Vijay Madanlal Choudhary v. Union of India (2022) SCC OnLine SC 929 – In a landmark judgment the Supreme Court upheld the constitutionality of key provisions of the *Prevention of Money-Laundering Act 2002*, including the reverse-burden clause under s.24 and the characterisation of money-laundering as a "continuing offence". This allowed the Enforcement Directorate to attach or confiscate assets—whether physical or digital—long after the predicate crime, provided the tainted proceeds were still being enjoyed. The ruling has empowered investigators to freeze crypto wallets and cloud-based ledgers linked to accounting fraud, materially strengthening NFRA's ability to coordinate with ED in complex technology-driven cases.

Shreya Singhal v. Union of India (2015) 5 SCC 1 – While the Court struck down s.66-A of the *IT Act 2000* for chilling free speech, it expressly upheld the surveillance and interception powers in Section 69. Forensic auditors now rely on court-sanctioned interceptions and

preserved e-mail trails collected under these provisions to prove intent and knowledge in digital-accounting-fraud prosecutions. The judgment thus narrowed over-broad criminalisation but preserved investigative tools vital to NFRA/ED joint probes.

CBI v. B. Rama Raju (Satyam Scam Prosecution, 2015) – The special CBI court admitted mirror-image copies of Satyam's Oracle financial database, together with server log files, as secondary electronic evidence under s.65-B of the *Evidence Act 1872*. This precedent validated full-disk imaging and hash verification as gold-standard techniques for preserving audit trails—techniques that NFRA now embeds in its Audit-Quality Reviews when red-flag anomalies are detected.

Foreign

United States v. Skilling 561 U.S. 358 (2010) – The U.S. Supreme Court limited the "honest-services" fraud statute to cover only bribery and kick-back schemes, yet affirmed Jeffrey Skilling's conviction for conspiring to deceive Enron's shareholders by manipulating digital accounting entries that hid massive losses. The case underscores how executive misrepresentations amplified by complex IT systems can still attract fraud liability, providing a comparative touchpoint for Indian courts interpreting managerial culpability in ERP-based manipulations.

Wirecard AG Insolvency Proceedings (Munich Regional Court, 2022 – ongoing) – German prosecutors allege that senior executives exploited a concealed back-door in Wirecard's SAP ledger to generate phantom cash balances held by third-party acquirers in Asia. The continuing trial has already prompted the European CEAOB (Committee of European Auditing Oversight Bodies) to issue cloud-audit guidance, emphasising log-file integrity and source-code access for auditors—principles NFRA can adopt when framing requirements for Indian issuers operating on offshore cloud platforms.

VI. INSTITUTIONAL ENFORCEMENT AND REGULATORY MECHANISMS

NFRA conducts Audit-Quality Reviews (AQRs) incorporating *Computer Assisted Audit Techniques* (CAATs) to parse 100% of transactional data. Where red flags emerge—unreconciled suspense entries; anomalous timestamp edits—NFRA may invoke Rule 7 to launch a suo-motu investigation, coordinate with SFIO for forensic imaging, and share intelligence with CERT-In for threat attribution.

Cross-Agency Coordination: NFRA collaborates with the Serious Fraud Investigation Office (SFIO), Enforcement Directorate (ED), and Income Tax authorities in multi-pronged

investigations involving digital fraud and money laundering.

VII. CHALLENGES IN ENFORCEMENT AND PROSECUTION

Data-localisation conflicts. Large Indian multinationals increasingly host ERP instances on hyperscale clouds based in Singapore or the US. Mutual-legal assistance procedures are slow, and foreign providers often require Mutual Legal Assistance Treaty (MLAT) orders before releasing audit logs, causing multi-quarter evidence gaps that perpetrators exploit to shred or overwrite data.

Acute shortage of cyber-forensic skills. Only about 2 per cent of practising chartered accountants in India hold CISA-level credentials. Audit files therefore rely heavily on management-supplied screenshots rather than independently scripted SQL extracts, undermining evidentiary robustness when fraud allegations surface.

Judicial backlog and procedural drift. Fraud cases under s 447 of the *Companies Act 2013* often languish in over-burdened special courts; average time to first charge-framing takes substantial time. This delay weakens witness memory and allows accused directors to dissipate proceeds via layered shell entities.

Encryption and compelled decryption lacunae. Full-disk and database-at-rest encryption—now default on major cloud platforms—renders hot-forensics impossible unless private keys are surrendered. Unlike the UK's RIPA s.49, the IT Act lacks explicit compelled-key disclosure provisions, leaving investigators hostage to voluntary cooperation.

Fragmented regulatory silos. NFRA, SEBI, RBI and SFIO each maintain separate whistle-blower portals and data lakes. Absence of a unified fraud-registry means cross-sector red flags (e.g., simultaneous receivables anomalies and suspicious banking transactions) are rarely stitched into a single investigative narrative.

Emerging technologies outpacing norms. Deep-fake documents generated by diffusion models can now mimic wet-ink signatures with near-pixel perfection. Current Indian Evidence Act provisions on electronic originals do not expressly address AI-synthesised artefacts, exposing a normative grey zone that defence counsel can exploit.

Limited whistle-blower protections. Section 177(9) of the Companies Act mandates a vigil mechanism, yet empirical studies show retaliation—demotion, litigation—remains common. Without strong anonymity shields and monetary incentives, insiders with first-hand knowledge of digital manipulations hesitate to approach regulatory bodies.

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

Cross-border asset-recovery hurdles. Fraud proceeds are increasingly routed through crypto mixers and parked in overseas SPVs. India lacks reciprocal recognition of confiscation orders with several key jurisdictions, forcing ED/NFRA to pursue protracted civil-litigation routes that erode asset value.

VIII. RECOMMENDATIONS AND THE WAY FORWARD

Legislative uplift – mandatory key-escrow for high-value databases. Amend the *Information Technology Act 2000* to mandate companies with annual turnover above ₹500 crore to maintain an encrypted "key-escrow" vault for every core accounting database. The escrow—held jointly by the statutory auditor, NFRA, and a government-notified cyber-trustee—would store de-cryption keys and hash-signatures of nightly back-ups. In the event of suspected fraud, regulators could rapidly unlock and image the entire ledger without relying on management co-operation, thereby reducing evidence-spoliation risk and expediting investigations under section 447 of the *Companies Act, 2013* and PMLA attachment proceedings.

NFRA Tech-Lab – AI-driven anomaly-scoring engine. Establish a dedicated *NFRA Technology Laboratory* staffed by data scientists, forensic accountants, and ethical hackers. The lab would build a cloud-native anomaly-scoring engine that ingests quarterly XBRL (eXtensible Business Reporting Language) filings, bank-statement feeds, and GST e-invoice data, then applies machine-learning models (e.g., Benford variance, unsupervised clustering & graph analytics) to flag irregularities in revenue recognition, related-party transactions, and journal-entry timing. High-risk scores would automatically trigger an Audit-Quality Review, enabling NFRA to shift from reactive investigations to predictive, risk-based supervision.

Auditor cyber-duty – Cyber Controls Assurance Report (CyCAR). Insert a new Rule under the *NFRA Rules 2018* requiring every statutory auditor of a listed or large unlisted entity to issue, alongside the traditional audit opinion, a *Cyber Controls Assurance Report* (CyCAR). Modeled on SOX s.404 internal-controls attestation, the CyCAR would evaluate the design and operating effectiveness of the client's cybersecurity controls over financial reporting—covering access management, change-log integrity, ransomware resilience, and third-party cloud contracts. Failure to obtain a clean CyCAR would necessitate a Key Audit Matter disclosure, enhancing board accountability and investor transparency.

Fast-track benches – specialised NCLT e-fraud courts. Create designated "e-fraud benches" within the National Company Law Tribunal, staffed by members trained in digital-evidence protocols and supported by a technical court officer cadre. These benches would hear matters

under ss 337–342 (misfeasance), s 447 (fraud), and NFRA disciplinary appeals on a 90-day writ timetable, using virtual-court infrastructure for real-time demonstration of forensic exhibits (hash values, log timelines, SQL-trace visualisations). Swift adjudication can reinforce deterrence and safeguard the value of seized digital assets from depreciation.

International MoUs – Cloud Act–style log-transfer pacts. India should pursue bilateral or multilateral agreements with key jurisdictions such as the US, EU, and Singapore—modeled on the U.S. CLOUD Act, 2018—to enable lawful, expedited access by NFRA and Indian law enforcement to offshore server logs, audit trails, and metadata. Such pacts should incorporate reciprocity, strict privacy safeguards, and judicial oversight, ensuring that cross-border evidence can be produced within statutory limitation periods while respecting data-protection standards such as GDPR Article 48.

IX. CONCLUSION

Digital accounting fraud represents a fast-moving, borderless threat that weaponizes code, cloud infrastructure and anonymised payment rails to subvert the very accounting architecture on which capital markets depend. Treating such misconduct as either a narrow audit deficiency or a siloed cyber incident fragments regulatory effort and leaves systemic blind spots. This study demonstrates that the only durable antidote is **regulatory convergence**—a seamless fusion of forensic-audit analytics, data-protection jurisprudence and extra-territorial cyber-law enforcement.

By mapping statutory gaps, analysing jurisprudence and benchmarking against PCAOB and ESMA praxis, the paper charts a concrete roadmap for upgrading NFRA from a post-factum inspector to a predictive, technology-driven sentinel. The recommended key-escrow mandate, AI-enabled anomaly engine, CyCAR reporting layer, specialised e-fraud benches and cross-border log-sharing pacts collectively re-imagine India's audit ecosystem for a US$ 5-trillion, cloud-native economy. Implemented in tandem, these reforms can shrink detection lags, harden internal controls, and restore global investor confidence in Indian financial reporting.

Ultimately, safeguarding the integrity of digital ledgers is not solely an accounting imperative; it is a constitutional and developmental one. As India accelerates towards digital-public-infrastructure leadership, NFRA's embrace of a tech-savvy, rights-respecting enforcement model can set a benchmark for emerging economies confronting the same protean risks.

*****

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

X. REFERENCES

1. *Companies Act*, 2013 (India).
2. *Information Technology Act*, 2000 (India), as amended in 2008.
3. *National Financial Reporting Authority Rules*, 2018 (India).
4. *Prevention of Money Laundering Act*, 2002 (India).
5. *Indian Evidence Act*, 1872, s. 65B, as amended in 2023.
6. *Sarbanes-Oxley Act*, 2002 (United States).
7. *Dodd-Frank Wall Street Reform and Consumer Protection Act*, 2010 (United States).
8. *General Data Protection Regulation*, Regulation (EU) 2016/679.
9. *Audit Regulation*, Regulation (EU) 537/2014.
10. *Fraud Act*, 2006 (United Kingdom).
11. *Regulation of Investigatory Powers Act*, 2000 (United Kingdom), s. 49.
12. *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, 2018 (United States).
13. *Vijay Madanlal Choudhary v. Union of India*, (2022) SCC OnLine SC 929.
14. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
15. *CBI v. B. Rama Raju (Satyam Scam)*, Special Court Order dated 09 April 2015.
16. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
17. *Pankaj Bansal v. Union of India*, (2023) SCC OnLine SC 1240.
18. *United States v. Skilling*, 561 U.S. 358 (2010).
19. *Munich Public Prosecutor v. Markus Braun (Wirecard)*, Regional Court of Munich, Case 27 Ks 1246/21 (proceedings pending).
20. E. Sutherland, *White Collar Crime* (Dryden Press, 1949).
21. R. Ramaswamy, *Corporate Frauds and Their Regulation in India* (LexisNexis, 2021).
22. M. Levi & N. Lord, *Fraud and Financial Crime* (Routledge, 2017).
23. P. Black & G. Kohler, *Digital Forensics for Accountants* (Wiley, 2020).
24. R. Jain & N. Agarwal, "Corporate Fraud and Money Laundering in India: Legal Framework and Judicial Trends" 10 *International Journal of Law & Policy Review* 44 (2023).

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]

25. J.C. Coffee, "Gatekeepers: The Professions and Corporate Governance" 84 *Virginia Law Review* 49 (1998).

26. J. Rubenfeld, "The Right to Privacy in the Digital Age" 30 *Yale Journal on Regulation* 3 (2013).

27. OECD, *Technology and Corporate Governance* (2022).

28. Institute of Chartered Accountants of India, *Forensic Accounting and Investigation Standards FAIS 110* (2023).

29. PCAOB, *Audit Quality Indicators Concept Release 2015 005* (2015).

30. European Securities and Markets Authority, *Report on the Enforcement of Financial Information* (2024) ESMA32 63 1527.

31. CEAOB, *Guidelines on Cloud Based Audit Procedures* (2023/05).

32. Ministry of Corporate Affairs (India), *NFRA Annual Report* (2023).

*****

© 2025. International Journal of Law Management & Humanities [ISSN 2581-5369]