IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Corporate Governance And Digital Fraud In India: A Legal Analysis Of Regulatory Mechanisms And Enforcement Gaps

Abishanth B. S1 and Dr. Sandeep S Desai2

1 LLM Student, Amity Law School, Amity University, Bengaluru.
1 Dean and Prof., Amity Law School, Amity University, Bengaluru.

ABSTRACT

In the rapidly evolving digital economy, the intersection of corporate governance and digital fraud has emerged as a pressing concern in India. As corporations increasingly adopt digital tools for financial transactions, data storage, and stakeholder communication, the risks of cyber-enabled frauds—including data breaches, insider manipulation, phishing, and financial misreporting—have grown exponentially. While corporate governance frameworks are designed to ensure accountability, transparency, and ethical business conduct, their effectiveness in detecting and preventing digital fraud remains inconsistent. This study provides a critical legal analysis of the existing regulatory mechanisms addressing digital fraud in the corporate sector and identifies enforcement gaps that undermine the resilience of India's corporate governance regime. The paper examines key statutes such as the Companies Act, 2013, the Information Technology Act, 2000, the SEBI (Listing Obligations and Disclosure Requirements) Regulations, and RBI guidelines, assessing their scope, overlaps, and limitations in curbing digital misconduct. It also explores the role of corporate boards, audit committees, compliance officers, and cybersecurity protocols in fostering a fraud-resistant corporate environment. Through the analysis of landmark cases and regulatory actions, the study highlights loopholes in internal control mechanisms, delayed responses to digital breaches, and inadequate penalties for non-compliance. Furthermore, the research explores comparative global practices, emphasizing the need for proactive governance strategies, real-time monitoring systems, and enhanced regulatory coordination between SEBI, RBI, CERT-In, and other enforcement bodies. It also stresses the importance of digital literacy and corporate accountability in addressing the behavioral and systemic dimensions of digital fraud. The study

[1] LLM Student, Amity Law School, Amity University, Bengaluru.
[2] Dean and Prof., Amity Law School, Amity University, Bengaluru.

concludes that while India has made notable strides in corporate governance reform, the regulatory response to digital fraud remains fragmented and reactive. Strengthening enforcement mechanisms, integrating digital risk management within governance frameworks, and fostering a culture of ethical technology use are crucial for safeguarding corporate integrity and investor confidence in the digital age.

KEYWORDS

Corporate governance, digital fraud, SEBI, corporate liability, compliance mechanisms.

INTRODUCTION

The intersection of corporate governance and digital fraud presents unique challenges in India's evolving business ecosystem. Indian corporations face unprecedented digitalization pressures alongside increasing fraud sophistication. Recent data reveals alarming trends in this domain with far-reaching implications for stakeholders.[3] The technological transformation has created novel opportunities for fraudulent activities.

Digital fraud incidents have multiplied exponentially across Indian financial institutions and corporates. Reserve Bank of India reported over 13,000 bank fraud cases in financial year 2024 alone.[4] More troubling are the statistics from the Ministry of Home Affairs revealing 1.1 million financial fraud cases registered during 2023. These incidents resulted in losses exceeding Rs. 7,488 crore.[5]

Account takeover attacks dominated the fraud landscape, accounting for approximately 55% of all digital fraud in India. Mule accounts represent another significant vulnerability in corporate banking systems. Third-party fraudsters gain access, establishing money movement networks that remain largely undetected.[6] Corporate security frameworks have struggled to address these evolving challenges.

India's digital transformation accelerated dramatically during 2020-2022, providing fertile ground for fraudulent activities. The nation's projected digital GDP should reach US$1 trillion by 2025, highlighting the growing economic stakes.[7] This rapid digitalization has outpaced governance frameworks and regulatory oversight mechanisms.

Corporate boards increasingly face pressure regarding technology oversight responsibilities. Many lack sufficient digital competence to evaluate management's control frameworks properly. A concerning Deloitte

[3] BioCatch Releases 2024 Digital Banking Fraud Trends in India, BioCatch, February 21, 2024, https://www.biocatch.com/press-release/biocatch-releases-2024-digital-banking-fraud-trends-report-in-india.
[4] India: number of bank fraud cases 2024, Statista, June 3, 2024, https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases/.
[5] Around 1.1 million financial fraud cases registered in 2023, shows data, Business Standard, February 6, 2024, https://www.business-standard.com/india-news/around-1-1-million-financial-fraud-cases-registered-in-2023-shows-data-124020601528_1.html.
[6] Report | 2024 Digital Banking Fraud Trends in India, BioCatch, https://www.biocatch.com/resources/white-paper/digital-banking-fraud-trends-india-2024.
[7] India's Digital Transformation, India-Briefing, https://www.india-briefing.com/doing-business-guide/india/sector-insights/india-digital-transformation.

survey revealed generative AI wasn't even on the agenda for 45% of Indian corporate boards.[8] This represents a significant governance blindspot.

This research paper contributes to emerging literature on technology governance and its relationship to corporate fraud prevention. Indian corporations demonstrate significant vulnerabilities where traditional governance models meet advanced digital threats. The findings hold implications for regulatory reform, corporate practice, and director responsibilities.[9] Better frameworks can mitigate these growing risks.

DIGITAL FRAUD IN THE INDIAN CORPORATE LANDSCAPE

Digital fraud refers to deceptive activities conducted through electronic systems that manipulate digital environments for illegal financial gain. The Information Technology Act, 2000 establishes the principal legal framework addressing such fraudulent activities in India. Section 43 of the Act specifically penalizes unauthorized access and data theft from computer systems. Digital fraud encompasses a broad spectrum of illicit activities beyond merely hacking, extending to sophisticated methods of deception that exploit technological vulnerabilities.[10]

Digital fraud can be classified based on various parameters including target, method, and impact. Target-based classification categorizes fraud as targeting individuals, corporations, financial institutions, or government bodies. Method-based classification focuses on techniques employed, such as phishing, malware deployment, social engineering, and credential theft. Impact-based classification examines whether the fraud results in financial loss, data breach, identity theft, or reputational damage. These classifications are not mutually exclusive, as complex digital frauds often incorporate multiple techniques targeting various entities simultaneously.[11]

The scope of digital fraud has expanded drastically with technological advancements. Initially limited to basic hacking and virus deployment, it now includes sophisticated attacks like ransomware, business email compromise, and deep fakes. The evolution coincides with the digital transformation of the Indian corporate sector, creating numerous vulnerabilities. The 2008 amendment to the Information Technology Act significantly broadened the scope by addressing emerging forms of cybercrimes. Section 66 now criminalizes fraudulent activities conducted electronically with penalties extending up to three years imprisonment and fines up to Rs. 5 lakhs for computer-related offences.[12]

---

[8] Top trends in corporate governance for 2025 & beyond, Diligent, https://www.diligent.com/resources/blog/corporate-governance-trends.
[9] Digital Transformation in the Indian Service Sector: Benefits, Challenges and Future Implications, ResearchGate, December 7, 2023, https://www.researchgate.net/publication/376307317_Digital_Transformation_in_the_Indian_Service_Sector_Benefits_Challenges_and_Future_Implications.
[10] Information Technology Act, 2000, Section 43.
[11] Cybersecurity Laws and Regulations Report 2025 India, International Comparative Legal Guides, November 6, 2024, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india.
[12] IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties, ClearTax, April 12, 2024, https://cleartax.in/s/it-act-2000.

- ***Common Types of Corporate Digital Frauds***

Phishing constitutes one of the most prevalent forms of digital fraud targeting corporations in India. This deceptive practice involves fraudsters impersonating legitimate entities to extract sensitive information such as login credentials or financial details. In the corporate context, sophisticated spear-phishing attacks target specific employees with access to valuable data or financial systems. According to recent statistics, over 8.5 lakh incidents of money loss and data breaches due to phishing have been documented in a two-year period, with losses exceeding Rs. 1,500 crores.[13]

Cyber fraud targeting payment systems poses a significant threat to Indian corporate environments. These include credit card fraud, ransomware attacks, and fraudulent transactions through compromised payment gateways. A notable case occurred in October 2016, when malware injection in Hitachi Payment Services system compromised approximately 3.2 million debit cards from major Indian banks. The National Payments Corporation of India reported losses of nearly Rs. 13 million through fraudulent transactions. Multiple banks including State Bank of India, HDFC, ICICI, and Axis Bank were severely affected, with SBI alone having to block and reissue 600,000 debit cards.[14]

Insider breaches represent a particularly dangerous form of corporate digital fraud because perpetrators exploit legitimate access to systems. These breaches occur when employees or contractors with authorized access misuse their privileges for financial gain or sabotage. Insider threats can be categorized as malicious insiders acting intentionally or negligent insiders who unknowingly enable breaches through carelessness or falling prey to social engineering. The Pune Citibank MphasiS Call Center Fraud exemplifies this risk, where ex-employees of MsourcE, the BPO arm of MphasiS Ltd, defrauded US Citibank customers of approximately Rs. 1.5 crores by exploiting their access to customer data.[15]

- ***Recent Cases and Trends in India***

The NSE co-location scam represents one of India's most significant digital fraud cases in recent years. This scandal involved the National Stock Exchange providing preferential access to its servers for certain brokers.[16] The scandal centered on OPG Securities, which exploited TCP/IP protocol vulnerabilities in the exchange's system architecture. Between 2010 and 2012, OPG Securities gained unethical advantages through faster data access via secondary server connections.[17]

The scandal came to light when a whistleblower alerted SEBI in 2015 about inequitable access to trading systems. Multiple investigations revealed that OPG Securities accessed the secondary server on 670 trading

[13] Phishing in India: All you need to know, LawBhoomi, July 21, 2023, https://lawbhoomi.com/phishing-in-india-all-you-need-to-know/.
[14] Data breaches in India, Wikipedia, December 14, 2024, https://en.wikipedia.org/wiki/Data_breaches_in_India.
[15] Cyber Crime Case Studies Ahmedabad :: Cyber Fraud In India, Cyber Legal Services, https://www.cyberralegalservices.com/detail-casestudies.php.
[16] NSE co-location scam, Wikipedia, November 5, 2024, https://en.wikipedia.org/wiki/NSE_co-location_scam.
[17] "NSE Co-location Scam: Everything You Need To Know!", GeeksforGeeks, July 28, 2023, https://www.geeksforgeeks.org/nse-co-location-scam-everything-you-need-to-know/.

days between 2010 and 2015. This gave them milliseconds advantage over competitors—critical in algorithmic trading environments.[18] Chitra Ramkrishna, former CEO of NSE, and Anand Subramanian, former Group Operating Officer, faced charges from the CBI for their alleged involvment in this breach of market integrity.[19]

The case's regulatory aftermath highlights persistent gaps in digital oversight. Despite the whistleblower's alert in 2015, substantial action took years to materialize. The Delhi High Court criticized the pace of investigation and questioned why effective action hadn't occurred earlier. SEBI finallt imposed penalties on NSE, but only in 2019, fining them approximately Rs. 11 billion ($131 million).[20]

September 2024 brought a significant development when SEBI dismissed charges against NSE and former officials. This dismissal cited “lack of sufficient evidence to prove collusion” despite acknowledging the exchange lacked “a detailed and defined policy” for co-location facilities. The reversal potentially removes obstacles for NSE's long-delayed public listing.[21]

Concurrent with the NSE case, major banking frauds exposed weaknesses in India's financial security architecture. The ABG Shipyard scandal emerged as India's largest banking fraud, surpassing Rs. 22,842 crore. This case involved diverting funds from a consortium of 28 banks, including ICICI and SBI.[22] The company allegedly engaged in complex financial manipulation, creating approximately 100 affiliates and associates to facilitate fraudulent transactions.[23]

The Punjab National Bank fraud involving Nirav Modi and Mehul Choksi exemplifies another sophisticated digital breach. This Rs 13,850 crore scam operated through fraudulent Letters of Undertaking issued via PNB's international banking system. The fraud went undetected between 2014 and 2017 because perpetrators manipulated the SWIFT messaging network while bypassing the bank's core banking solution.[24]

Digital banking fraud continues its upward trajectory in India. The Reserve Bank of India documented over 13,000 bank fraud cases in financial year 2024 alone. This marks significant increase over previous years, reflecting greater vulnerability as digital banking adoption expands.[25] The trend shows evolution toward more

[18] NSE co-location scam: Delhi HC asks CBI to file affidavit mentioning status, Business Standard, February 15, 2023, https://www.business-standard.com/article/current-affairs/nse-co-location-scam-delhi-hc-asks-cbi-to-file-affidavit-mentioning-status-123021501124_1.html.
[19] CBI arrests Sanjay Gupta, main accused in NSE co-location scam case, Business Standard, June 22, 2022, https://www.business-standard.com/article/markets/cbi-arrests-sanjay-gupta-main-accused-in-nse-co-location-scam-case-122062200252_1.html.
[20] NSE Co-Location Scam: CBI Raids Properties Linked To Chitra Ramkrishna, India.com, May 21, 2022, https://www.india.com/business/nse-co-location-scam-case-latest-cbi-raids-properties-linked-to-chitra-ramkrishna-investigate-traders-brokers-anand-subramanian-mysterious-yogi-5404613/.
[21] India market regulator dismisses charges against NSE in 2019 co-location case, Reuters, September 13, 2024, https://www.reuters.com/markets/asia/india-market-regulator-dismisses-charges-against-nse-2019-colocation-case-2024-09-13/.
[22] From Nirav Modi to ABG Shipyard: Why do bank frauds keep happening in India?, Scroll.in, February 26, 2022, https://scroll.in/article/1017952/why-bank-frauds-like-the-rs-22800-crore-abg-shipyard-scam-keep-happening-in-india.
[23] Yet another bank fraud: Bigger and different, Business Standard, February 20, 2022, https://www.business-standard.com/article/opinion/yet-another-bank-fraud-bigger-and-different-122022000885_1.html.
[24] What is PNB Scam, Business Standard, May 10, 2025, https://www.business-standard.com/about/what-is-pnb-scam.
[25] India: number of bank fraud cases 2024, Statista, June 3, 2024, https://www.statista.com/statistics/1012729/india-number-of-bank-fraud-cases/.

technologically sophisticated attacks utilizing social engineering, synthetic identities, and payment system vulnerabilities.

LEGAL AND REGULATORY FRAMEWORK IN INDIA

- ***Companies Act, 2013: Governance Obligations and Director Duties***

The Companies Act, 2013 marks a watershed moment in Indian corporate governance. It attempts to cure the deficiencies present in the previous 1956 legislation. Director obligations have been meticulously outlined in Section 166. This codification brings more certainty and accountability to board members. Directors must act based on the company's Articles of Association at all times. They need to work in good faith to support stakeholder interests and promote company objects. They should exercise independent judgment with reasonable care, skill, and diligence. Conflicts of interest must be avoided or disclosed promptly. The directors cannot take undue advantage of their position. The act prohibits activities that may lead to loss of independent decision-making power.[26]

Section 166 applies to all types of directors including independent ones. Such provisions foster corporate governance through efficient management practices. Directors must resolve corporate issues swiftly with mature decision-making approaches. Personal interests must take a backseat to company and stakeholder interests. Financial statement fraud involves manipulating financial records to show fake prosperity. Such practices undermine business integrity and damage investor confidence. Satyam Computer Services scandal, often called “India's Enron,” represents one of the most notorious cases of corporate fraud. Ramalinga Raju, the company's founder and chairman, admitted to inflating company revenue by $1.47 billion, shocking the business community and causing investor panic.[27]

The Companies Act, 2013 makes directors personally liable for fraudulent activities. Section 447 defines fraud in relation to company affairs comprehensively. It includes acts, omissions, fact concealment, or position abuse committed by any person with intent to deceive. The punishment is imprisonment ranging from six months to ten years alongside fines. Directors' duties extend beyond mere financial oversight. They have an obligation to maintain transparency in board proceedings. They must disclose personal interests in contracts or proposed arrangements. Confidentiality of sensitive information must be protected diligently. They need to take steps to prevent insider trading activities. The Act mandates timely and accurate financial reporting by directors to ensure a true picture of company finances.[28]

[26] Arunava Bandyopadhyay, “Duties of Directors under the Indian Companies Act, 2013,” iPleaders Blog, October 10, 2019, https://blog.ipleaders.in/directors-duties/.
[27] “Unmasking Corporate Frauds in India,” IDfy, March 21, 2025, https://www.idfy.com/blog/unmasking-corporate-frauds-in-india/.
[28] “Rights, Liabilities And Duties of Directors Under Indian Companies Act, 2013,” Legal Service India, accessed May 15, 2025, https://www.legalserviceindia.com/legal/article-6448-rights-liabilities-and-duties-of-directors-under-indian-companies-act-2013.html.

- ***SEBI (LODR) Regulations: Compliance and Disclosure Requirements***

Securities and Exchange Board of India's Listing Obligations and Disclosure Requirements (LODR) Regulations form a vital regulatory framework. They ensure comprehensive corporate governance in listed entities. The regulations mandate timely and transparent disclosures to stakeholders. SEBI introduced these regulations in 2015 to consolidate various disclosure requirements. The LODR mandate governs a company from the time it becomes listed through its operational conduct. It aims to ensure business transparency, promote better governance, protect investor interests, and standardize disclosure requirements. Digital adoption in enforcement has become increasingly important.[29]

SEBI's LODR Regulations work in conjunction with the Companies Act to enforce robust governance. Listed companies must maintain an optimal mix of executive and non-executive directors. At least half of board members must be non-executive directors. At least one woman director is mandatory. For corporate governance, SEBI mandates quarterly financial results disclosure. Companies must report income statements, balance sheets, and cash flow details. Annual reports must include management discussion and analysis sections. Material events like mergers, acquisitions, or major litigation need immediate disclosure. Related party transactions require shareholder approval and detailed reporting.[30]

SEBI enforces strict penalties for non-compliance with LODR provisions. The enforcement mechanisms include fines, trading suspensions, and freezing promoter shareholding. Serious violations may lead to debarment of directors from capital markets. The regulations require companies to file compliance reports on corporate governance periodically. These reports detail adherence to board composition rules, committee functioning, and disclosure compliance. The LODR framework has undergone several amendments to address evolving market dynamics. Recent changes strengthen compliance for related party transactions and material event disclosures.[31]

Corporate fraud incidents have significantly shaped India's regulatory landscape. The Nirav Modi-PNB fraud case involving around INR 15,000 crores pushed regulatory improvements. After this scam, the government approved the Fugitive Economic Offenders Bill. It allows confiscation of assets including Benami holdings of absconding loan defaulters. The Infrastructure Leasing & Financial Services (IL&FS) fraud, amounting to INR 91,000 crores, showed governance lapses even in companies backed by major institutions like LIC and SBI. The fraud occurred mainly through diversion of borrowed money by senior management members. It led to tightened regulatory scrutiny of systemically important financial institutions.[32]

[29] "Understanding SEBI's Listing Obligations and Disclosure Requirements (LODR) Mandate," IRIS Business, February 19, 2025, https://irisbusiness.com/an-in-depth-look-at-sebis-listing-obligations-and-disclosure-requirements-lodr-mandate/.
[30] "SEBI Amendments to the LODR – An Overview of Key Changes," India Corporate Law, July 4, 2023, https://corporate.cyrilamarchandblogs.com/2023/07/sebi-amendments-to-the-lodr-an-overview-of-key-changes/.
[31] "Corporate Governance Laws and Regulations Report 2024-2025 India," ICLG, July 15, 2024, https://iclg.com/practice-areas/corporate-governance-laws-and-regulations/india.
[32] Minhaj Nazeer, "All about corporate fraud," iPleaders, February 12, 2024, https://blog.ipleaders.in/all-about-corporate-fraud/.

- ***Information Technology Act, 2000: Cybersecurity and Data Protection***

The Information Technology Act, 2000 (IT Act) stands as India's primary legislation governing digital interactions. It provides legal recognition to electronic records and digital signatures. The Act facilitates electronic governance and grants validity to online contracts. It establishes a framework for addressing cybercrimes and outlines penalties for violations. Section 43A imposes liability on corporations for failure to protect sensitive data. Companies must implement reasonable security practices to safeguard personal information. Failure to protect such data makes them liable to pay compensation to affected individuals.[33]

The IT Act underwent significant amendment in 2008 to address emerging cybersecurity challenges. It introduced provisions for data protection and privacy in the digital realm. The amendment added Section 66A that penalized sending "offensive messages" though later struck down. It also incorporated Section 69, which empowered authorities to monitor digital information. These changes reflect the evolving nature of digital threats and regulatory responses. The Act also established the framework for digital signatures, ensuring security and authentication in online transactions. Companies and LLPs under the MCA21 e-Governance program must utilize digital signatures for document filing.[34]

The IT Act addresses cybercrime through various provisions targeting different types of malicious activities. It defines and penalizes offenses such as hacking, identity theft, and cyber terrorism. Section 66 specifically deals with computer-related offenses including unauthorized access and data theft. Section 66F addresses cyber terrorism with stringent penalties including life imprisonment. Section 67 prohibits publishing obscene material in electronic form. These provisions aim to create a secure digital environment for individuals and businesses alike. The Act however lacks comprehensive provisions for domain name disputes and intellectual property protection.[35]

- ***Role of RBI and CERT-In in Corporate Digital Risk Management***

The Reserve Bank of India (RBI) plays a pivotal role in managing digital risks in financial sector. RBI issues guidelines for cybersecurity and fraud prevention in digital transactions. It mandates banks and financial institutions to implement robust security measures. The Master Direction on Digital Payment Security Controls, 2021 introduces comprehensive standards. These directions cover governance, risk management and security controls. Financial entities must follow common minimum standards regardless of their size or nature. The RBI focuses on both preventive measures and incident response mechanisms. It continually updates guidelines to address emerging threats in digital payment ecosystem.[36]

[33] "Information Technology Act, 2000," iPleaders Blog, August 24, 2022, https://blog.ipleaders.in/information-technology-act-2000/.
[34] "IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties," ClearTax, April 12, 2024, https://cleartax.in/s/it-act-2000.
[35] "Information Technology Act, 2000," Wikipedia, March 26, 2025, https://en.wikipedia.org/wiki/Information_Technology_Act,_2000.
[36] "The Latest RBI Guideline to Make Digital Transactions Safe," Bajaj Finserv, April 12, 2022, https://www.bajajfinserv.in/latest-rbi-guideline-to-make-digital-transactions-safe.

RBI's guidelines extend to data localization for enhanced security and sovereignty. In April 2018, RBI directed payment firms to store all transaction data on servers in India. The circular titled 'Storage of Payment System Data' set a six-month compliance deadline. Payment system operators must ensure end-to-end transaction details remain within Indian territory. This includes customer data, payment credentials, and transaction information. Cross-border processing remains permissible, but data must be deleted from overseas systems within 24 hours. The policy aims to facilitate regulatory oversight and protect citizens' financial information. Compliance involves regular audits and certification by qualified professionals.[37]

CERT-In (Indian Computer Emergency Response Team) serves as the national agency for cybersecurity. Established under Section 70B of the IT Act, CERT-In coordinates incident response activities. It functions under the Ministry of Electronics and Information Technology (MeitY). Its primary responsibilities include cybersecurity incident detection, analysis, and response. CERT-In issues advisories regarding vulnerabilities and emerging threats. It conducts regular security drills and exercises to assess preparedness. The agency also provides technical assistance to organizations facing security breaches. CERT-In emerged as the central coordination point in India's cybersecurity ecosystem.[38]

Corporate entities must report cybersecurity incidents to CERT-In within strict timeframes. The agency's 2022 directive mandates reporting incidents within six hours of detection. Organizations must maintain ICT system logs within Indian territory for effective investigation. They must synchronize system clocks with specified Network Time Protocol servers. CERT-In can request information from any service provider, intermediary, or data center. Non-compliance with these directives attracts penalties under the IT Act. The stringent reporting requirements aim to enhance national cybersecurity posture. They also enable timely intervention and minimize damage from cyber attacks.[39]

CORPORATE GOVERNANCE AS A PREVENTIVE TOOL AGAINST DIGITAL FRAUD

- ***Key Principles: Transparency, Accountability, Risk Oversight***

Transparency forms the bedrock of robust corporate governance frameworks designed to combat digital fraud. Indian corporate law mandates disclosure of material information to stakeholders at regular intervals. The Companies Act, 2013 significantly strengthened transparency requirements across both listed and unlisted entities.[40] This principle extends beyond mere financial disclosures to encompass related party transactions, risk factors, and governance structures.

[37] "RBI Data Localisation - Everything you need to know about RBI's data localization guidelines," AppSealing, June 5, 2023, https://www.appsealing.com/rbi-data-localization/.
[38] "Indian Computer Emergency Response Team," Wikipedia, May 12, 2025, https://en.wikipedia.org/wiki/Indian_Computer_Emergency_Response_Team.
[39] "Understanding Computer Emergency Response Team (CERT-In): India's Cybersecurity Response Framework," India Law, November 25, 2024, https://www.indialaw.in/blog/civil/cert-in-india-cybersecurity-framework/.
[40] Corporate Governance, Drishti IAS, https://www.drishtiias.com/to-the-points/paper4/corporate-governance-1.

Accountability mechanisms create clear lines of responsibility within corporate structures. Board members bear fiduciary duties toward shareholders and other stakeholders. The Kumar Mangalam Birla Committee's recommendations, incorporated into SEBI regulations, established accountability standards for Indian corporations.[41] These include board composition requirements, audit committee responsibilities, and mandate to create effective internal control systems to detect digital fraud.

Risk oversight has evolved as a cornerstone principle in corporate governance. The Companies Act, 2013 requires boards to develop and implement risk management policies. Section 134(3)(n) specifically mandates directors to include statements in their reports identifying risks that could threaten company existence.[42] Digital risks have gained prominence with the proliferation of technology-enabled transactions in Indian business operations.

Corporate governance serves as both preventive and detective mechanism against digital fraud. Principles like fair dealing and ethical conduct extend beyond legal compliance. The National Guidelines for Responsible Business Conduct (NGRBC) released by Ministry of Corporate Affairs in 2019 adopted Gandhian trusteeship principles. These guidelines aim to balance profit-making with broader social responsibilities.[43] This ethical dimension proves especially crucial in cyberspace where regulations often lag behind technological advancements.

- ***Role of Audit Committees, Independent Directors, and Internal Controls***

Audit committees serve as financial watchdogs with significant fraud prevention functions. Section 177 of the Companies Act, 2013 mandates their establishment for listed entities and specific categories of public companies. These include companies with paid-up capital exceeding Rs.10 crore, turnover above Rs.100 crore, or outstanding loans/deposits beyond Rs.50 crore.[44] Their composition requirements ensure objective oversight, with independent directors forming the majority.

Audit committees possess expansive mandates extending beyond traditional financial oversight. Their responsibilities include examining financial statements, evaluating internal financial controls, and scrutinizing related party transactions. The committee reviews whistleblower reports pertaining to financial misconduct or digital fraud. Section 177(9) specifically tasks audit committees with establishing vigilance mechanisms within organizational structures.[45] This vigilance function becomes essential in detecting technology-enabled frauds that often escape conventional detection methods.

[41] Principles of Corporate Governance: The Indian Perspective, The Law Brigade Publishers, September 26, 2019, https://thelawbrigade.com/company-law/principles-of-corporate-governance-the-indian-perspective/.
[42] Corporate Governance Laws and Regulations Report 2024-2025 India, ICLG, July 15, 2024, https://iclg.com/practice-areas/corporate-governance-laws-and-regulations/india.
[43] Corporate Governance Reforms in India: SEBI's Role in Enhancing Transparency and Accountability, The Amikus Qriae, May 12, 2024, https://theamikusqriae.com/corporate-governance-reforms-in-india-sebis-role-in-enhancing-transparency-and-accountability/.
[44] Audit Committee under Section 177 of Companies Act,2013, TaxGuru, February 23, 2019, https://taxguru.in/company-law/audit-committee-section-177-companies-act2013.html.
[45] Section 177. Audit Committee, Companies Act Integrated Ready Reckoner, https://ca2013.com/177-audit-committee/.

Independent directors play critical roles in preventing digital fraud through objective oversight. Companies Act, 2013 Section 149(4) requires listed companies to have at least one-third of board positions filled by independent directors. These directors must possess ability to read and understand financial statements, ensuring capacity to identify financial red flags potentially indicating fraud.[46] Their independence from management creates crucial checks and balances within governance structures.

The independent director's role extends beyond passive oversight to active fraud prevention. They bear responsibility for approving related party transactions, chairing audit committees, and ensuring whistleblower mechanism effectiveness. SEBI regulations enhance these responsibilities by requiring independent directors to evaluate non-independent directors' performance, assess information flow quality, and review management's compliance with board recommendations.[47] Their detachment from operational management creates valuable objectivity in assessing digital fraud risks.

- ***Whistleblower Policies and Fraud Reporting Mechanisms***

Whistleblower policies create structured pathways for reporting suspected digital fraud without fear of retaliation. Section 177(9) of Companies Act, 2013 makes establishment of vigil mechanisms mandatory for listed companies and certain other entities. These mechanisms must protect individuals making genuine disclosures about unethical behavior, actual or suspected fraud, or violations of company codes of conduct.[48] Effective implementation remains uneven across Indian corporations despite these legal mandates.

The statutory framework for whistleblowing shows progressive evolution. Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014 provides specific guidelines for implementing vigil mechanisms. The Audit Committee typically oversees these mechanisms, with direct access provided to the chairperson in exceptional cases. Repeated frivolous complaints may attract reprimands. The Whistleblower Protection Act, though introduced, has faced implementation challenges and coverage limitations.[49] Private sector employees particularly lack comprehensive protections compared to public sector counterparts.

SEBI has strengthened whistleblower provisions for listed entities through amendments to LODR regulations. These amendments mandate implementation of whistleblower policies with adequate safeguards against victimization. Companies must disclose policy details on their websites and in board reports. SEBI's 2019 amendment specifically targeted insider trading by establishing incentive structures for whistleblowers

[46] Gatekeepers of Governance – Audit Committee, India Corporate Law, December 12, 2022, https://corporate.cyrilamarchandblogs.com/2022/06/regulatory-overload-on-audit-committees-is-there-a-need-to-have-a-fresh-look-at-its-role/.
[47] Importance of Corporate Governance and Independent Directors in India, Lexology, October 11, 2023, https://www.lexology.com/library/detail.aspx?g=f7074e5e-bfc9-46d6-abd0-bc1cf531d131.
[48] Whistleblowing Policy in India | The Law and Challenges, MyAdvo, https://www.myadvo.in/blog/whistleblowing-policy-in-india-the-law-and-challenges/amp/.
[49] Whistleblowing in India: Are we there yet?, Nishith Desai Associates, https://www.nishithdesai.com/SectionCategory/33/White-Collar-and-Investigations-Practice/12/52/WhiteCollarandInvestigationsPractice/4426/1.html.

reporting such violations.[50] The maximum reward under this scheme reaches Rs 1 crore, creating meaningful financial motivation for reporting serious securities violations.

Fraud reporting mechanisms must balance accessibility with confidentiality protections. Effective systems include multiple reporting channels, clear investigation protocols, and appropriate escalation procedures. The CARO 2020 significantly enhanced focus on whistleblower complaints. It requires statutory auditors to consider all whistleblower complaints received during financial year review. Auditors must evaluate management's handling of complaints and assess financial implications.[51] This creates an external accountability layer for complaint processing.

- ***Codes of Conduct and Ethical Compliance***

Codes of conduct establish behavioral expectations for directors, executives, and employees interacting with digital systems. The Companies Act, 2013 mandates senior management adherence to code provisions. These codes typically address conflicts of interest, confidentiality obligations, and fair dealing requirements. SEBI has progressively strengthened code of conduct requirements through LODR regulation amendments.[52] These amendments particularly target digital misconduct including data misappropriation, algorithmic manipulation, and digital piracy.

Ethical compliance extends beyond legal requirements to incorporate socially responsible practices and stakeholder considerations. The Companies Act, 2013 recognizes this through Section 135, which mandates Corporate Social Responsibility activities. The National Guidelines for Responsible Business Conduct further articulate ethical expectations beyond statutory requirements.[53] Organizations with strong ethical cultures demonstrate greater resistance to digital fraud through collective commitment to integrity and transparent operations.

Compliance monitoring depends on both preventative and detective controls integrated throughout organizational structures. These include regular training programs, attestation requirements, and technological safeguards against unauthorized activities. Companies must establish clear oversight responsibilities, typically through compliance officers or committees with direct board reporting lines. Audit trails for digital transactions create accountability mechanisms that deter fraudulent activities.[54] Effective compliance systems blend technological protections with human oversight to address evolving digital vulnerabilities.

[50] The Indian Disposition On Whistleblowing In A Private Company, Mondaq, November 4, 2021, https://www.mondaq.com/india/directors-and-officers/1128912/the-indian-disposition-on-whistleblowing-in-a-private-company.
[51] Fraud Reporting under Companies Act vis-à-vis Whistleblower Mechanism, S.S. Rana & Co., April 19, 2024, https://ssrana.in/articles/fraud-reporting-companies-act-whistleblower-mechanism/.
[52] Code of Conduct, IoD, December 10, 2024, https://www.iod.com/resources/governance/code-of-conduct/.
[53] Comparison of 8 Major Companies' Code of Ethics and Conduct, Polonious Systems, August 30, 2023, https://www.polonious-systems.com/blog/code-of-ethics-and-conduct/.
[54] Code of Ethics: Understanding Its Types and Uses, Investopedia, https://www.investopedia.com/terms/c/code-of-ethics.asp.

COMPARATIVE PERSPECTIVE AND GLOBAL BEST PRACTICES

- ***Digital Fraud Governance in the US***

The United States pioneered robust corporate governance reforms through the Sarbanes-Oxley Act. Enacted in July 2002, SOX emerged as a direct response to major corporate scandals. Companies like Enron, WorldCom, and Tyco International had undermined investor confidence through fraudulent practices. The legislation introduced sweeping changes to corporate governance standards across America. It established the Public Company Accounting Oversight Board to regulate auditors. SOX imposes stringent requirements for financial reporting accuracy and transparency in public companies. It covers crucial issues like auditor independence, internal control assessment, and enhanced financial disclosure.[55]

Section 404 represents the most significant SOX provision for fraud prevention in digital environments. It requires extensive internal control testing and documentation by public companies. Management must evaluate and report on internal control effectiveness annually. External auditors must attest to the accuracy of management's assessment. This creates multiple layers of accountability for financial reporting systems. The focus on system-level controls specifically addresses emerging digital fraud vulnerabilities. The provision has significantly strengthened corporate defenses despite initial implementation costs. Financial reporting has become more reliable though continuous monitoring remains challenging.[56]

SOX Section 302 establishes personal liability for corporate officers regarding financial reporting. CEOs and CFOs must personally certify the accuracy of financial statements. This signature requirement changes the risk calculation for executives contemplating fraudulent activities. Criminal penalties for violations include up to 25 years imprisonment for securities fraud. The possibility of personal criminal liability serves as a powerful deterrent against digital manipulation. Personal accountability extends to oversight of internal controls and fraud prevention systems. Executives must certify they've disclosed significant control deficiencies to auditors.[57]

The SOX implementation experience offers valuable lessons for digital fraud prevention globally. Initial compliance efforts revealed widespread control weaknesses in information technology systems. Companies discovered vulnerability to digital manipulation throughout their financial reporting ecosystems. This led to increased investment in automated monitoring tools and cybersecurity enhancements. Organizations subsequently reported unexpected benefits beyond mere compliance. These included strengthened control

[55] "Sarbanes-Oxley Act," Wikipedia, April 12, 2025, https://en.wikipedia.org/wiki/Sarbanes–Oxley_Act.
[56] "The Effects of the Sarbanes-Oxley Act of 2002," Investopedia, accessed May 16, 2025, https://www.investopedia.com/ask/answers/052815/what-impact-did-sarbanesoxley-act-have-corporate-governance-united-states.asp.
[57] "Sarbanes-Oxley Act: What It Does to Protect Investors," Investopedia, accessed May 16, 2025, https://www.investopedia.com/terms/s/sarbanesoxleyact.asp.

environments, more reliable documentation, and standardized IT processes. The enhanced transparency has created lasting improvements in fraud detection capabilities.[58]

- ***UK Corporate Governance Code and Cyber Compliance***

The UK Corporate Governance Code establishes principles-based standards for listed companies. Published by the Financial Reporting Council, it follows a "comply or explain" approach. The 2024 Code represents the most recent revision with significant cybersecurity enhancements. It applies to financial years beginning on or after January 1, 2025. The Financial Conduct Authority requires companies in the commercial and closed-ended investment fund categories to follow it. Companies must disclose areas of non-compliance and provide substantive explanations. The flexible principles-based approach encourages adaptation to emerging digital threats.[59]

The 2024 Code introduces significant provisions addressing digital fraud and cybersecurity governance. It requires outcomes-based governance reporting focusing on board decisions and impacts. Companies must assess and monitor how their desired corporate culture gets embedded. Boards must provide an annual declaration regarding the effectiveness of material controls. These controls specifically include digital systems protecting against cyber fraud. A new Provision 29 mandates enhanced monitoring of internal control frameworks. The revisions reflect growing awareness of cyber risk as a material governance concern.[60]

The Financial Conduct Authority plays a central role in UK cybersecurity compliance oversight. It monitors adherence to the Corporate Governance Code through company reporting reviews. The FCA issues specific guidance on cybersecurity risk management for financial services firms. This guidance emphasizes board accountability for cyber resilience and fraud prevention. The regulator conducts periodic cyber resilience assessments across the financial sector. It also employs supervisory technology to detect control weaknesses in regulated entities. The FCA can impose substantial penalties for governance failures enabling digital fraud.[61]

- ***OECD Guidelines on Corporate Governance***

The Organization for Economic Co-operation and Development provides influential governance standards. The G20/OECD Principles of Corporate Governance serve as global benchmarks. First published in 1999, they've undergone significant revisions to address digital risks. The Principles help policymakers evaluate and improve corporate governance frameworks. They identify key building blocks for sound governance systems

[58] "The Unexpected Benefits of Sarbanes-Oxley," Harvard Business Review, April 1, 2006, https://hbr.org/2006/04/the-unexpected-benefits-of-sarbanes-oxley.
[59] "UK Corporate Governance Code," Financial Reporting Council, accessed May 16, 2025, https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/.
[60] "New UK Corporate Governance Code – getting ready for the changes," White & Case LLP, accessed May 16, 2025, https://www.whitecase.com/insight-alert/new-uk-corporate-governance-code-getting-ready-changes.
[61] "Understanding the UK Corporate Governance Code: The Complete Guide," AuditBoard, accessed May 16, 2025, https://auditboard.com/blog/understanding-the-uk-corporate-governance-code-the-complete-guide.

worldwide. International financial institutions use them as standards for sound market practices. The 2023 version incorporates substantial digital risk management elements.[62]

The OECD Principles emphasize six core areas relevant to digital fraud prevention. They promote effective corporate governance frameworks through appropriate legal structures. They address shareholder rights and equitable treatment including protection from abuse. The Principles recognize stakeholder interests in sustainable corporate performance. They mandate disclosure and transparency regarding all material corporate matters. They establish clear board responsibilities for strategic guidance and management oversight. These foundational elements create resilience against emerging digital threats.[63]

The OECD specifically addresses technology governance through dedicated guidance on digital issues. Companies should conduct thorough due diligence on technology development, sale, and use. This includes assessment of potential misuse scenarios even by legitimate customers. Organizations must enhance transparency around data access and sharing practices. They should adopt responsible data governance including privacy safeguards and ethical principles. The guidelines recommend protections against consumer manipulation and coercion through digital means. OECD guidance increasingly addresses algorithmic governance and AI system controls.[64]

FINDINGS AND REFORM SUGGESTIONS

The regulatory framework addressing digital fraud reflects significant fragmentation across multiple authorities. SEBI, RBI, and Ministry of Corporate Affairs operate with varying degrees of coordination. This creates regulatory arbitrage opportunities exploited by sophisticated fraudsters crossing jurisdictional boundaries.[65] Certain digital fraud categories fall through regulatory cracks entirely.

Corporate governance reforms post-Satyam scandal strengthened financial oversight but failed to anticipate tech-enabled frauds. The Kotak Committee recommendations in 2018 belatedly addressed some digital vulnerabilities. These included stricter independence criteria and enhanced whistleblower protections.[66] Implementation remains inconsistent across market segments.

Risk assessment methodologies show crucial deficiencies regarding digital threats. Most corporate boards lack competence in cybersecurity and digital operations. This creates dangerous knowledge gaps when

[62] "G20/OECD Principles of Corporate Governance 2023," OECD, accessed May 16, 2025, https://www.oecd.org/en/publications/g20-oecd-principles-of-corporate-governance-2023_ed750b30-en.html.
[63] "ComplianceOnline Dictionary- OECD Principles of Corporate Governance," ComplianceOnline, accessed May 16, 2025, https://www.complianceonline.com/dictionary/OECD_Principles_of_Corporate_Governance.html.
[64] "The OECD Guidelines and technology," OECD Watch, November 8, 2023, https://www.oecdwatch.org/oecd-ncps/the-oecd-guidelines-for-mnes/what-is-in-the-oecd-guidelines/the-oecd-guidelines-and-technology/.
[65] Corporate Governance Laws and Regulations Report 2024-2025 India, ICLG, July 15, 2024, https://iclg.com/practice-areas/corporate-governance-laws-and-regulations/india.
[66] Evolution of Corporate Governance in India, LawBhoomi, January 11, 2025, https://lawbhoomi.com/evolution-of-corporate-governance-in-india/.

evaluating management's digital risk mitigation strategies.[67] Independent directors often accept technology claims without adequate scrutiny.

Whistleblower mechanisms demonstrate improving design but suffer from implementation failures. Theoretical protections exist in law without practical safeguards for those reporting digital misconduct. Enforcement data shows low reporting rates and even lower successful prosecutions from whistleblower complaints.[68] This undermines confidence in reporting systems.

Board accountability structures require substantial strengthening to address digital fraud challenges. Directors face minimal personal consequences for governance failures enabling major frauds. The Companies Act theoretically establishes director liability. Enforcement actions rarely target oversight failures by board members.[69] This weakens deterrence.

The RBI Cybersecurity Framework provides critical guidance but lacks comprehensive enforcement mechanisms. Banks must implement 24/7 Security Operations Centers and real-time monitoring systems. However, compliance verification remains procedural rather than substantive.[70] This creates paper-based compliance without meaningful security improvements.

Technology adoption timelines for security enhancements should be accelerated across the financial sector. Legacy systems create persistent vulnerabilities exploited by fraudsters. Regulatory safe harbors could incentivize modernization investments.[71] Security-by-design principles must inform all financial technology deployments.

CONCLUSION

India's corporate governance framework has evolved significantly in response to digital fraud challenges. The regulatory landscape shows measured progress yet exhibits persistent gaps. Key legislations present a foundation for governance structures and accountability mechanisms. Yet these laws often struggle to keep pace with evolving digital threats. The Companies Act, 2013 and SEBI regulations represent substantive improvements over their predecessors. However, their enforcement remains inconsistent across different sectors and company sizes.[72]

Recent statistics paint a troubling picture of digital fraud proliferation in India. Trading scams alone cost Indians over ₹1,420 crore between January and April 2024. The Indian Computer Emergency Response Team reports that account takeover attacks constitute approximately 55% of all fraud. Data from 2024 indicates

[67] Corporate Governance, Drishti IAS, https://www.drishtiias.com/to-the-points/paper4/corporate-governance-1.
[68] Unmasking Corporate Frauds in India, IDfy, March 21, 2025, https://www.idfy.com/blog/unmasking-corporate-frauds-in-india/.
[69] Corporate Governance, State Bank of India, https://sbi.co.in/corporate/AR1920/coporate-governance.html.
[70] RBI Guidelines for Cybersecurity Framework, Sectona, January 30, 2025, https://sectona.com/technology/rbi-guidelines-for-cybersecurity-framework/.
[71] RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16, https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721.
[72] "India's Corporate Governance Reforms: 2023 Year Roundup List," India Briefing, December 30, 2023, https://www.india-briefing.com/news/indias-corporate-governance-reforms-key-regulatory-changes-to-pay-attention-to-in-2024-30677.html/.

annual losses due to cyber fraud have exceeded ₹1.7 billion. These figures underscore the immense financial toll of inadequate corporate governance safeguards.[73]

Technological vulnerabilities continue to expose corporate entities to significant risks. Mobile payment fraud presents particular concerns given UPI's widespread adoption. Identity-based fraud exploits gaps in digital identity verification systems. PwC's Financial and Cyber Fraud Survey 2024 identifies weak internal controls as major contributors. Limited investments in governance protocols further exacerbate cyber fraud incidents. Organizations often lack robust frameworks for monitoring and response.[74]

Corporate boards demonstrate varying levels of digital risk awareness and oversight capability. PwC's 2024 Digital Trust Insights reveals only partial board engagement with emerging technologies. Generative AI remains absent from 45% of corporate board agendas. This represents a significant blindspot in governance oversight. Modern boards must incorporate technology expertise to effectively monitor digital risks. Director qualifications increasingly need to include digital literacy components.[75]

International standards offer valuable frameworks adaptable to Indian corporate governance needs. SOX principles regarding personal accountability can strengthen India's corporate officer liability requirements. UK emphasis on board-level cybersecurity governance addresses SEBI regulation gaps. OECD principles on disclosure and transparency complement existing Indian reporting standards. Selective adoption allows India to benefit from global best practices while respecting local conditions.[76]

Looking forward, India's regulatory evolution must accelerate to match digital transformation pace. Corporate governance regulations need technology-specific provisions for emerging risks. SEBI's LODR requirements should expand to include detailed cybersecurity governance standards. The Companies Act might benefit from amendments addressing digital fraud specifically. Board evaluation criteria should incorporate digital risk oversight capabilities. Corporate governance education must integrate technological dimensions more thoroughly.[77] India's path toward robust digital fraud governance requires multi-stakeholder commitment. Corporate leaders must champion governance beyond mere compliance orientations. Regulators need to develop more agile and responsive oversight mechanisms. Technology providers should incorporate governance features into product designs. Investors increasingly must evaluate governance quality regarding digital risks. The intersection of corporate governance and digital fraud prevention represents a critical frontier for India's economic security.[78]

[73] "Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024," Business Standard, May 27, 2024, https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html.
[74] "Financial and Cyber Fraud Report 2024," Grant Thornton Bharat, accessed May 16, 2025, https://www.grantthornton.in/insights/financial-and-cyber-fraud-report-2024/.
[75] "Top trends in corporate governance for 2025 & beyond," Diligent, accessed May 16, 2025, https://www.diligent.com/resources/blog/corporate-governance-trends.
[76] "Cyber Governance Code of Practice," GOV.UK, April 7, 2025, https://www.gov.uk/government/publications/cyber-governance-code-of-practice.
[77] "Cybersecurity In India: 2024 Global Digital Trust Insights Survey," PwC India, accessed May 16, 2025, https://www.pwc.in/digital-trust-insights-india.html.
[78] "Cyber Security in Corporate Governance," Legal Service India, accessed May 16, 2025, https://www.legalserviceindia.com/legal/article-559-cyber-security-in-corporate-governance.html.