

Cyber Fraud, Digital Evidence, and Corporate Governance: Reconstructing Forensic Accountability in the Fourth Industrial Revolution

Dr. Gaduga Godwin, Esq

Lecturer at Accra Institute of Technology Adjunct Lecturer at Blue Crest University College

ABSTRACT	ARTICLE DETAILS
The migration of economic life onto digital infrastructure has transformed the character of occupational and organizational fraud while leaving the architecture of corporate accountability largely unreformed. This article examines the widening gap between cyber fraud, whose perpetrators exploit the velocity, anonymity, and jurisdictional fluidity of networked systems, and the governance and evidentiary frameworks through which organizations are expected to detect wrongdoing, preserve proof, and assign responsibility. Drawing on fraud theory, agency theory, and the scholarship of digital forensics, the article synthesizes recent empirical evidence, including the Association of Certified Fraud Examiners (2024) global study of 1,921 cases across 138 countries and the Federal Bureau of Investigation (2025) internet crime data recording USD 16.6 billion in reported losses for 2024, to demonstrate that conventional internal control and audit mechanisms were designed for a paper economy and translate imperfectly to an algorithmic one. It then develops the concept of forensic accountability, defined as the institutionalized capacity of an organization to generate, preserve, and produce reliable digital evidence of its own conduct and of misconduct against it, and argues that this capacity should be treated as a core governance obligation of boards rather than a technical residue delegated to information technology departments. The article proposes an integrated framework linking fraud risk management, forensic readiness, and board oversight, and considers its practical implications for regulators, audit committees, forensic practitioners, and educators in both developed and developing jurisdictions.	Published On: 15 August 2026
KEYWORDS: Cyber Fraud, Digital Evidence, Corporate Governance, Forensic Accounting, Forensic Readiness, Fourth Industrial Revolution, Accountability	Available on: https://ijiissh.com/

INTRODUCTION

Fraud has always adapted to the technologies of its time, and the ledger, the cheque, the telegraph, and the telephone each produced its own generation of schemes together with its own generation of controls. What distinguishes the present moment, which Schwab (2016) characterized as the Fourth Industrial Revolution, is not merely the arrival of another instrument of deception but the fusion of digital, physical, and biological systems into a single economic substrate on which value is created, transferred, and recorded. When the corporate enterprise itself becomes a network of databases, application programming interfaces, cloud tenancies, and automated decision systems, the traditional distinction between the business and its information technology dissolves, and with it dissolves the comfortable assumption that fraud can be managed through periodic audit of documents that exist somewhere in a filing cabinet.

The empirical record suggests that this transformation has been asymmetric, favouring offenders over the institutions charged with restraining them. The Association of Certified Fraud Examiners (ACFE, 2024), in the thirteenth edition of its global study, analyzed 1,921 cases of occupational fraud drawn from 138 countries and territories, with total identified losses exceeding USD 3.1 billion and a median loss of USD 145,000 per case, and reaffirmed its long-standing estimate that the typical organization loses about five percent of annual revenue to fraud. In the same period, the Federal Bureau of Investigation (FBI, 2025) reported that complaints to its Internet Crime Complaint Center in 2024 produced USD 16.6 billion in reported losses, an increase of thirty-three percent over the previous year, with cyber-enabled fraud accounting for roughly eighty-three percent of the total and business email compromise alone generating losses of approximately USD 2.77 billion. These figures understate the true incidence of the problem, since much fraud is never detected and much detected fraud is never reported (Button & Cross, 2017; Levi & Burrows, 2008), yet even as

conservative floors they describe an environment in which digital deception has become one of the most consequential categories of economic crime in the world.

The scholarly and professional response to this environment has developed along three largely separate tracks. Criminologists and fraud examiners have refined explanatory models of offender behaviour, extending Cressey's (1953) fraud triangle into the fraud diamond and beyond (Wolfe & Hermanson, 2004; Free, 2015; Lokanan, 2015). Computer scientists and forensic technologists have built an elaborate discipline of digital evidence handling, codified in international standards and national guidelines (Casey, 2011; International Organization for Standardization [ISO], 2012; Kent et al., 2006). Corporate governance scholars, for their part, have debated board composition, audit committee effectiveness, and internal control frameworks within a literature whose foundational concerns predate the commercial internet (Cadbury, 1992; Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013; Jensen & Meckling, 1976). Each track has matured, but the connective tissue among them remains thin. Boards approve cyber security budgets without understanding whether the systems they fund can produce evidence admissible in court, forensic examiners recover artefacts from systems whose retention policies were never designed with litigation in mind, and auditors certify control frameworks that say little about what happens after a breach or a defalcation is discovered.

This article addresses that disconnection. Its central claim is that the Fourth Industrial Revolution requires a reconstruction of accountability itself, and that the organizing concept for this reconstruction should be what the article terms forensic accountability: the institutionalized capacity of an organization to generate, preserve, and produce reliable digital evidence of its own conduct and of misconduct committed against it or within it. Forensic accountability is broader than cyber security, which concerns the prevention of intrusion, and broader than forensic readiness as conventionally defined in the technical literature (Rowlingson, 2004), because it locates the evidentiary capability within the governance structure of the firm and treats it as an obligation of directors rather than a preference of technicians. The argument proceeds in six stages. The article first sets out its conceptual and theoretical foundations, then maps the anatomy of cyber fraud in the contemporary economy, examines the law and science of digital evidence, analyses the governance gap that separates board oversight from forensic capability, develops the integrated framework of forensic accountability, and finally draws out practical implications for regulators, practitioners, and educators before acknowledging limitations and directions for future research.

CONCEPTUAL AND THEORETICAL FRAMEWORK

Fraud Theory in a Digital Register

The dominant explanatory account of fraud remains the triangle that Cressey (1953) distilled from his interviews with convicted embezzlers, in which a non-shareable financial pressure, a perceived opportunity, and a rationalization converge to produce the violation of trust. Wolfe and Hermanson (2004) added a fourth element, capability, on the reasoning that many frauds require a perpetrator with the position, intelligence, and confidence to recognise an opening and exploit it over time. Subsequent scholarship has qualified these models, noting that they were built on the confessions of individual offenders and travel awkwardly to collusive, organizational, and predatory frauds (Free, 2015; Lokanan, 2015), and Sutherland's (1949) older insight that white collar crime is learned within business cultures rather than born of individual pathology remains an essential corrective to purely individualist accounts.

Digitalization does not overturn these models so much as it redistributes weight among their elements. Opportunity, in Cressey's scheme, was constrained by physical access to assets and records, whereas in a networked enterprise opportunity is a function of credentials, privileges, and the porousness of interfaces, and it can be manufactured remotely by an offender who has never entered the building and owes the organization no fiduciary duty at all. Capability, similarly, can now be rented, since phishing kits, ransomware affiliates, and money mule networks allow offenders of modest technical skill to deploy sophisticated attacks (Button & Cross, 2017). Rationalization is eased by distance, because a perpetrator who manipulates a payment instruction from another continent never sees the payroll clerk who is dismissed for the resulting shortfall. The consequence is that the population of potential offenders against any given organization has expanded from its own employees and close counterparties to, in principle, anyone with a connection to the internet, while the internal population retains all of its traditional motives and has acquired new instruments. The ACFE (2024) data illustrate the persistence of the internal threat: asset misappropriation still appeared in eighty-nine percent of occupational fraud cases, corruption in nearly half, and financial statement fraud, though present in only five percent of cases, produced the highest median loss at USD 766,000.

Agency Theory and the Problem of Verification

Corporate governance scholarship begins from the separation of ownership and control and the agency costs that separation generates (Fama & Jensen, 1983; Jensen & Meckling, 1976). Principals cannot directly observe the conduct of agents, so they invest in monitoring devices, of which the statutory audit, the independent board, and the internal control system are the most institutionalized examples. Beasley (1996) demonstrated empirically that firms with a higher proportion of outside directors were less likely to experience financial statement fraud, a finding that anchored decades of reform aimed at board independence, and the

succession of governance codes from the Cadbury Report (1992) through the G20/OECD Principles of Corporate Governance (Organization for Economic Co-operation and Development [OECD], 2023) has progressively elaborated the monitoring apparatus. Agency theory, however, presupposes that monitoring is technically possible, that the records an agent generates can be inspected and that inspection will reveal deviation. Power (1997) observed that the audit society tends to verify auditable surrogates rather than underlying realities, and digitalization sharpens his point considerably. When transactions are executed by algorithms, approved through workflows whose logs sit in third-party clouds, and settled in seconds across borders, the surrogates available for inspection are themselves digital artefacts whose integrity depends on the very systems under scrutiny. The verification problem at the heart of agency theory therefore becomes, in the Fourth Industrial Revolution, an evidentiary problem: the principal's capacity to hold the agent accountable is only as good as the organization's capacity to produce trustworthy digital records of what the agent did. This is the theoretical junction at which governance scholarship and digital forensics meet, and it is the junction this article occupies.

The Fourth Industrial Revolution as Context

Schwab (2016) described the Fourth Industrial Revolution as distinct from its predecessors in velocity, scope, and systemic impact, marked by technologies such as artificial intelligence, ubiquitous connectivity, distributed ledgers, and the internet of things that blur the boundaries between the digital and the physical. For present purposes, three features of this environment matter most. First, the evidentiary substrate of commerce has become volatile: data that would once have persisted in ledgers for decades may now be overwritten in days by routine log rotation unless someone decides to preserve it. Second, the perimeter of the firm has become notional, since employees, contractors, suppliers, and software services interpenetrate one another's systems continuously. Third, decision-making itself is increasingly delegated to models whose reasoning is difficult to reconstruct after the fact, which complicates both the commission and the investigation of fraud. Each feature strains a governance architecture that still assumes stable records, defined boundaries, and human decision-makers who can be examined under oath.

THE ANATOMY OF CYBER FRAUD IN THE FOURTH INDUSTRIAL REVOLUTION

Typologies and Scale

Cyber fraud is best understood not as a single offence but as a family of schemes united by their dependence on digital systems for execution, concealment, or monetization. At one end of the family sit the high-volume social engineering frauds. Phishing and spoofing generated 193,407 complaints to the Internet Crime Complaint Center in 2024, more than any other category, and business email compromise, in which offenders impersonate executives, suppliers, or advisers to redirect legitimate payments, produced 21,442 complaints and approximately USD 2.77 billion in reported losses in the same year (FBI, 2025). At the other end sit frauds that exploit the financial infrastructure of the digital economy itself, including investment frauds that accounted for roughly USD 6.57 billion in reported losses in 2024 and the rapidly growing category of cryptocurrency-enabled schemes, which the FBI (2025) associated with about USD 9.3 billion in losses, an increase of some sixty-six percent over the prior year. Between these poles lie ransomware and extortion, payroll and vendor master-file manipulation, synthetic identity fraud, and the manipulation of automated decision systems.

Occupational fraud, the misuse of one's position for personal enrichment, has meanwhile been reshaped rather than replaced. The ACFE (2024) found that the median scheme still runs for about twelve months before detection, that tips remain the leading detection mechanism at forty-three percent of cases, and that more than half of all cases were associated with an absence of internal controls or the override of controls that existed. Perpetrator seniority remains the strongest predictor of loss severity, with frauds by owners and executives producing a median loss of USD 500,000 against USD 60,000 for ordinary employees. What has changed is the medium: the fraudulent journal entry is now a database record, the forged invoice is a portable document generated in seconds, and the concealment that once required physical destruction of documents can be accomplished, or attempted, through deletion, encryption, and the quiet alteration of logs. The convergence of external cyber offenders and internal occupational offenders on the same digital terrain is the defining condition of contemporary fraud risk.

Why Digital Environments Favour Offenders

Four structural properties of digital environments explain the asymmetry between attack and defence. The first is velocity, since funds moved by instantaneous payment systems or converted into crypto assets can be layered beyond practical recovery within hours, whereas investigation, freezing orders, and mutual legal assistance operate on timescales of weeks to years. The second is scalability, because a scheme that once required an offender to deceive victims one at a time can now be executed against thousands simultaneously at negligible marginal cost. The third is jurisdictional arbitrage, in that offenders deliberately route conduct through states with weak enforcement capacity or without extradition arrangements, a difficulty the Council of Europe (2001) Convention on Cybercrime and the African Union (2014) Convention on Cyber Security and Personal Data Protection were designed to mitigate but which persists wherever ratification and implementation lag. The fourth, and for this article the most important, is evidentiary fragility: the proof of a digital fraud consists of volatile artefacts, including logs, metadata, memory contents, and network captures,

that decay or disappear unless deliberately preserved, so that the offender's concealment strategy is often assisted by the victim organization's own indifference to retention (Casey, 2011; Garfinkel, 2010).

These properties interact with organizational psychology in ways that governance frameworks rarely acknowledge. Victim organizations frequently prefer quiet remediation to reporting, whether to protect reputation, avoid regulatory attention, or simply to move on, and this preference suppresses the collective intelligence on which deterrence depends (Button & Cross, 2017). The result is a market failure in information: each firm underinvests in evidence and disclosure because the benefits of prosecution and systemic learning accrue largely to others, while the costs of preservation, investigation, and candour fall on itself. Correcting that failure is, in substantial part, what a doctrine of forensic accountability is for.

DIGITAL EVIDENCE: INTEGRITY, ADMISSIBILITY, AND THE CHAIN OF CUSTODY

The Science of Digital Forensics

Digital forensics has developed from an improvised craft into a discipline with articulated principles, and its canonical process, comprising identification, collection, acquisition, and preservation followed by analysis and reporting, is codified in ISO/IEC 27037 (ISO, 2012) and elaborated for organizational incident response in the guidance of the United States National Institute of Standards and Technology (Kent et al., 2006). The discipline's central commitments are that original evidence should be altered as little as possible and only by competent persons for documented reasons, that every action taken upon evidence should be recorded so that an independent expert could evaluate and, where appropriate, replicate it, and that the integrity of acquired data should be demonstrable, typically through cryptographic hashing, from the moment of acquisition to the moment of presentation (Casey, 2011). The chain of custody, the documented and unbroken record of who held what evidence, when, where, and for what purpose, is the procedural spine that connects these commitments to legal proceedings.

Garfinkel (2010) warned that the golden age of digital forensics, in which examiners could image a single hard disk and reconstruct a user's conduct with high fidelity, was ending under the pressure of encryption by default, cloud storage, the proliferation of devices, and the sheer volume of data, and the intervening years have vindicated the warning. Evidence relevant to a modern corporate fraud is scattered across endpoint devices, enterprise applications, software-as-a-service platforms whose logs are controlled by third parties, mobile devices subject to personal privacy expectations, and messaging services designed to leave no trace. Artificial intelligence complicates the picture further, both as an instrument of fraud, as in deepfake-enabled impersonation of executives (FBI, 2025), and as a challenge to authentication, since the ease of generating synthetic documents, voices, and video erodes the default credibility that courts and investigators once extended to recordings and images. The forensic question of the coming decade is less whether an artefact can be recovered than whether its provenance can be proved.

Admissibility and the Legal Architecture

Legal systems have converged on a functional approach to electronic evidence, admitting it where its reliability, integrity, and provenance can be established rather than excluding it for want of an original paper form. In the United States, expert forensic testimony must satisfy the reliability standards articulated in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993), which direct courts to consider testability, error rates, peer review, and general acceptance, a framework that has pushed digital forensic practice toward documented methodology and validated tools. Statutory schemes in many jurisdictions perform the complementary task of equalizing electronic and paper records: Ghana's Electronic Transactions Act, 2008 (Act 772), for example, provides for the admissibility of electronic records and directs attention to the reliability of the manner in which the record was generated, stored, and communicated, and the country's Cybersecurity Act, 2020 (Act 1038) establishes institutional machinery for incident response and the protection of critical information infrastructure. At the regional and international level, the Council of Europe (2001) Convention on Cybercrime harmonizes procedural powers such as expedited preservation of stored data, and the African Union (2014) Malabo Convention, which entered into force in 2023, extends a comparable framework across a continent whose digital economies are among the fastest growing in the world.

The practical significance of this architecture for corporations is easily stated and widely ignored: admissibility is manufactured, or forfeited, long before litigation begins. A court asked to rely on an audit log will want to know how the log was generated, whether the clock that timestamped it was synchronized, who had administrative rights to alter it, and how the copy before the court is shown to be identical to the original, and the answers to those questions are determined by decisions about system configuration, retention, and access control taken years earlier by people who never imagined a courtroom. An organization that cannot answer them has not merely a weak case but, in a real sense, no institutional memory that the law can credit. This is the precise point at which evidence law becomes a governance concern, because only the board and senior management can mandate, fund, and sustain the enterprise-wide practices on which future admissibility depends.

CORPORATE GOVERNANCE AND THE ACCOUNTABILITY GAP

The Inherited Control Architecture

The modern apparatus of corporate accountability was assembled in response to the corporate scandals of the twentieth century. The Cadbury Report (1992) articulated the board's responsibility for internal control and the audit committee's oversight role, COSO (2013) supplied the dominant internal control framework organised around control environment, risk assessment, control activities, information and communication, and monitoring, and the Sarbanes-Oxley Act of 2002 hardened these expectations into law for issuers in the United States, requiring executive certification of disclosures under section 302 and management assessment of internal control over financial reporting under section 404. COSO (2017) subsequently reframed risk oversight as integral to strategy and performance, and the G20/OECD Principles were revised in 2023 to give explicit attention to digitalization and sustainability in governance (OECD, 2023). In Africa, the King IV Report (Institute of Directors in Southern Africa, 2016) is notable for going further than most codes, dedicating a distinct principle to the governance of technology and information and directing boards to treat both as strategic assets requiring their oversight.

This inheritance is substantial, but it was built to answer a particular question, namely whether financial statements are reliable, and its instruments, including segregation of duties, authorization hierarchies, reconciliations, and periodic audit, presume that the records subject to control are stable and that deviation will leave inspectable traces. The presumption fails in characteristic ways in digital environments. Segregation of duties collapses when a single compromised administrator credential confers the powers of many roles at once. Authorization hierarchies are bypassed when the fraudulent instruction arrives through the authentic email account of the authorizer. Reconciliation detects the diversion of funds only after the money has crossed three borders. Periodic audit, sampling transactions months in arrears, is structurally incapable of catching schemes whose entire lifecycle, from intrusion to monetization, may span seventy-two hours. None of this renders the inherited architecture useless, and the ACFE (2024) evidence that fraud losses are substantially lower where anti-fraud controls exist confirms its continuing value, but it does mean that the architecture no longer suffices.

The Missing Evidentiary Dimension

What the inherited architecture most conspicuously lacks is an evidentiary dimension. Governance codes instruct boards to oversee risk management and internal control, and increasingly to oversee cyber security, but they are largely silent on whether the organization can prove anything: whether its systems generate records of adequate integrity, whether those records are retained for periods matching limitation statutes and investigative realities, whether an incident can be investigated without destroying the evidence it leaves behind, and whether the organization could, if required, place before a court or regulator a trustworthy account of its own digital conduct. Rowlingson (2004) named this capability forensic readiness and framed it as maximizing the environment's ability to collect credible digital evidence while minimizing the cost of investigations, yet two decades later forensic readiness remains, in most organizations, a technical aspiration buried in information security policy rather than a governance obligation visible to the board.

The consequences of this omission surface predictably after major incidents. Investigations stall because logs were rotated before anyone thought to preserve them, and disciplinary and criminal proceedings collapse. After all, the chain of custody cannot be reconstructed, insurance claims are contested because the insured cannot substantiate the mechanism of loss, and regulators impose sanctions less for the breach itself than for the organization's inability to explain it, a dynamic reinforced by regimes such as the European Union's General Data Protection Regulation (2016), whose article 33 obliges controllers to notify personal data breaches within seventy-two hours and to document breaches in a manner that permits verification of compliance. In each instance, the underlying failure is the same: evidence was treated as an incidental by-product of operations rather than as an asset whose creation and preservation the governing body is responsible for assuring. Closing that gap is not a matter of purchasing forensic software; it is a matter of reconstructing accountability.

RECONSTRUCTING FORENSIC ACCOUNTABILITY: AN INTEGRATED FRAMEWORK

Defining Forensic Accountability

Forensic accountability, as this article conceives it, is the institutionalized capacity of an organization to generate, preserve, and produce reliable digital evidence of its own conduct and of misconduct committed within it or against it, sustained by governance structures that assign responsibility for that capacity to the board and senior management. The concept integrates three bodies of practice that currently operate in isolation. From fraud risk management, it takes the discipline of anticipating schemes and designing controls around the elements of pressure, opportunity, rationalization, and capability (Cressey, 1953; Wolfe & Hermanson, 2004). From digital forensics, it takes the principles of evidence integrity, documented handling, and defensible methodology (Casey, 2011; ISO, 2012; Kent et al., 2006). From corporate governance, it takes the mechanisms of board oversight, delegated committee responsibility, and disclosure through which organizational capacities are directed and verified (COSO, 2013; OECD, 2023). The distinctive claim is that evidentiary capability is not a technical property of systems but a governance property of institutions, in the

same way that financial reporting quality came to be understood, after the reforms of the early 2000s, as a property of the control environment rather than of the bookkeeping alone.

The Architecture of the Framework

The framework operates at four connected levels. At the level of the board, forensic accountability requires that oversight of fraud risk and evidentiary capability be assigned explicitly, whether to the audit committee, a risk committee, or a dedicated technology governance committee on the model encouraged by King IV (Institute of Directors in Southern Africa, 2016), and that the board receive periodic assurance not only that defences exist but that the organization has tested its ability to investigate itself. Directors need not become technologists, but they must be able to ask, and insist on answers to, a small set of decisive questions: what evidence do our critical systems generate, how long is it kept, who can alter it, how quickly can it be preserved under legal hold, and when did we last rehearse an investigation from detection through to a report that would withstand adversarial scrutiny.

At the level of management systems, the framework requires a forensic readiness programme integrated with enterprise risk management rather than appended to information security. Its elements are familiar from the technical literature (Rowlingson, 2004) but acquire new force when mandated from above: an evidence inventory mapping the systems whose records matter for the organization's principal fraud scenarios; retention schedules reconciled with limitation periods, regulatory requirements, and investigative experience; logging and time synchronization standards that make records mutually corroborating; preservation and legal hold procedures that can be triggered within hours; documented arrangements with cloud and platform providers guaranteeing access to logs and cooperation in investigations; and relationships with law enforcement and external forensic specialists established before they are needed. The ACFE (2024) finding that tips detect more fraud than any other mechanism, and that organizations with reporting hotlines suffer substantially smaller losses, argues for treating whistleblowing channels as part of the evidentiary system, since a tip is often the event that starts the preservation clock.

At the level of the assurance professions, forensic accountability implies an expanded mandate. Internal audit should test not only whether controls prevent fraud but whether the organization could prove a fraud if one occurred, auditing log integrity, retention compliance, and the operability of preservation procedures as it now audits reconciliations. External auditors, whose responsibilities regarding fraud are defined by standards such as International Standard on Auditing 240 (International Auditing and Assurance Standards Board [IAASB], 2009), inevitably confront digital evidence whenever they respond to identified fraud risks, and the reliability of the electronic records underlying the financial statements is increasingly inseparable from the reliability of the statements themselves. Forensic accountants and examiners, finally, are the natural translators between the technical and governance registers, and their professional formation should equip them to advise boards on evidentiary capability as fluently as they now testify about loss quantification (Kranacher & Riley, 2019).

At the level of the legal and regulatory environment, the framework depends on convergence between what courts require and what organizations build. Statutes on electronic transactions and cybercrime, from Act 772 and Act 1038 in Ghana to the instruments of the Council of Europe (2001) and the African Union (2014), define the demand side of forensic accountability by specifying what reliable electronic evidence looks like and what procedural powers investigators hold, while governance codes and listing rules define the supply side by specifying what boards must oversee and disclose. Regulators can accelerate convergence by treating demonstrated forensic readiness as a mitigating factor in enforcement, much as effective compliance programmes are treated in sentencing frameworks, thereby giving boards a concrete incentive to invest in capability whose benefits are otherwise realized only in the aftermath of misfortune.

Forensic Accountability in Developing and Emerging Economies

The framework carries particular significance for developing and emerging economies, where digital financial services have expanded faster than the institutional capacity to police them. Mobile money platforms, instant payment systems, and rapidly digitizing public administrations have brought millions into the formal economy across Africa, Asia, and Latin America while simultaneously creating dense new surfaces for fraud, and the regional data are sobering: the ACFE (2024) reported median losses in Sub-Saharan Africa and other developing regions comparable to, and in some regions exceeding, those in North America, notwithstanding far shallower pools of forensic expertise. In such settings, the temptation is to import cybersecurity technology while deferring the slower work of evidentiary institution-building, yet the ordering should arguably be reversed, because prosecutions, asset recovery, and public trust in digital systems all depend on evidence that courts will accept. Instruments such as the Malabo Convention (African Union, 2014) and national statutes such as Ghana's Cybersecurity Act, 2020 (Act 1038) provide the legal skeleton; forensic accountability, adopted as a governance norm by boards, regulators, and professional bodies, supplies the musculature. There is also a pedagogical implication, since universities and professional institutes in these jurisdictions train the auditors, lawyers, and examiners who will operate the framework, and curricula that continue to separate evidence law, information systems, and governance into non-communicating silos reproduce precisely the disconnection this article criticizes.

Practical and Policy Implications

For boards and audit committees, the immediate implication is agenda reform. Fraud and evidentiary capability should appear as standing items supported by management reporting that goes beyond incident counts to address preservation capacity, investigation outcomes, and lessons implemented, and directors should commission periodic independent assessments of forensic readiness with the same seriousness they bring to financial statement audit. Charters of audit and risk committees should be amended to name evidentiary capability expressly, since responsibilities that are nobody's in particular have a documented tendency to be nobody's at all.

For practitioners, the implications are methodological. Forensic accountants and fraud examiners should incorporate evidentiary capability assessment into fraud risk assessments, asking of each significant scheme scenario not only how it would be prevented and detected but how it would be proved, and incident responders should internalize the discipline that containment decisions taken in the first hours of a breach, such as re-imaging compromised machines, are frequently the destruction of the case. Legal advisers, for their part, should participate in the design of retention and preservation regimes rather than encountering them for the first time in discovery, and should press cloud and platform contracts for audit and cooperation clauses while bargaining power still exists.

For regulators and standard setters, three moves suggest themselves. The first is to articulate forensic readiness expectations within corporate governance codes, following the direction indicated by King IV's treatment of technology and information governance (Institute of Directors in Southern Africa, 2016) and the OECD's (2023) attention to digitalization, so that comply-or-explain and apply-and-explain regimes generate disclosure about evidentiary capability. The second is to align breach notification, record retention, and electronic evidence statutes so that organizations face coherent rather than contradictory duties, a task of particular urgency where data protection regimes mandating minimization coexist uneasily with investigative regimes rewarding preservation. The third is to invest in the public forensic infrastructure, including accredited laboratories, judicial training in digital evidence, and mutual legal assistance capacity, without which private forensic accountability terminates at the courtroom door.

For educators, finally, the article implies curricular integration. Accounting programmes should teach digital evidence handling alongside audit sampling, law faculties should treat electronic evidence and cyber fraud as core rather than elective, and information systems programmes should expose future engineers to the legal afterlife of the logs their architectures generate or fail to generate. The professionals who will operate the Fourth Industrial Revolution's accountability systems are being trained now, and they will reproduce either the silos or the synthesis.

LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

This article is conceptual, and its claims invite empirical testing. The framework of forensic accountability rests on a synthesis of secondary evidence, principally the global datasets of the ACFE (2024) and the FBI (2025), whose limitations are well understood: both depend on reported and investigated cases, both undercount frauds that victims conceal or never discover, and cross-jurisdictional comparisons are complicated by differences in reporting propensity and legal definition (Levi & Burrows, 2008). Future research could operationalize forensic readiness as a measurable organizational construct and examine its association with investigation outcomes, loss recovery, regulatory treatment, and even cost of capital, thereby subjecting the article's central claim, that evidentiary capability is value-relevant governance, to falsification. Comparative institutional work is also needed on how boards in different governance traditions, from the unitary Anglo-American model to two-tier and stakeholder-oriented systems, assimilate evidentiary oversight, and on whether the apply-and-explain philosophy of King IV produces richer disclosure of forensic capability than comply-or-explain regimes. Finally, the evidentiary consequences of artificial intelligence, including the authentication of synthetic media and the auditability of algorithmic decisions implicated in fraud, constitute an open frontier at which law, forensic science, and governance scholarship will be obliged to meet again.

CONCLUSION

The Fourth Industrial Revolution has not abolished fraud; it has re-platformed it. Offenders internal and external now operate on the same digital terrain, exploiting velocity, scale, jurisdictional fluidity, and, above all, the evidentiary fragility of systems that were engineered for performance rather than proof. The governance apparatus inherited from the twentieth century, for all its achievements, addresses this terrain obliquely, overseeing controls whose assumptions the terrain has dissolved while remaining silent on the organization's capacity to establish, credibly and admissibly, what actually happened. This article has argued that the silence should end, and that the organizing concept for ending it is forensic accountability: the treatment of reliable digital evidence as a governed institutional capacity, mandated by boards, embedded in management systems, tested by assurance professionals, and rewarded by regulators. The reconstruction it proposes is demanding, since it asks directors to extend their oversight into territory conventionally ceded to technicians, asks professions to redraw their curricula and methodologies, and asks legislatures and regulators to align statutes that grew up separately. It is, however, the demand the moment makes. An economy that records everything and can prove almost nothing is an invitation to impunity, and the answer to it lies not in any single technology but in the older and harder work of building institutions that can be believed.

REFERENCES

- 1) African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection*. <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>
- 2) Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. <https://legacy.acfe.com/report-to-the-nations/2024/>
- 3) Beasley, M. S. (1996). An empirical analysis of the relation between the board of directors' composition and financial statement fraud. *The Accounting Review*, 71(4), 443–465.
- 4) Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge. <https://doi.org/10.4324/9781315679877>
- 5) Cadbury, A. (1992). *Report of the Committee on the Financial Aspects of Corporate Governance*. Gee Publishing.
- 6) Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.
- 7) Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework*. COSO.
- 8) Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management—Integrating with strategy and performance*. COSO.
- 9) Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>
- 10) Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.
- 11) Cybersecurity Act, 2020 (Act 1038) (Ghana).
- 12) Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
- 13) Electronic Transactions Act, 2008 (Act 772) (Ghana).
- 14) Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The Journal of Law and Economics*, 26(2), 301–325. <https://doi.org/10.1086/467037>
- 15) Federal Bureau of Investigation, Internet Crime Complaint Center. (2025). *2024 internet crime report*. U.S. Department of Justice. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
- 16) Free, C. (2015). Looking through the fraud triangle: A review and call for new directions. *Meditari Accountancy Research*, 23(2), 175–196. <https://doi.org/10.1108/MEDAR-02-2015-0009>
- 17) Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7(Suppl.), S64–S73. <https://doi.org/10.1016/j.diin.2010.05.009>
- 18) Institute of Directors in Southern Africa. (2016). *King IV report on corporate governance for South Africa 2016*. IoDSA.
- 19) International Auditing and Assurance Standards Board. (2009). *International Standard on Auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements*. International Federation of Accountants.
- 20) International Organization for Standardization. (2012). *Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC Standard No. 27037). <https://www.iso.org/standard/44381.html>
- 21) Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- 22) Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-86>
- 23) Kranacher, M.-J., & Riley, R. A. (2019). *Forensic accounting and fraud examination* (2nd ed.). Wiley.
- 24) Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK: A conceptual and empirical journey. *The British Journal of Criminology*, 48(3), 293–318. <https://doi.org/10.1093/bjc/azn001>
- 25) Lokanan, M. E. (2015). Challenges to the fraud triangle: Questions on its usefulness. *Accounting Forum*, 39(3), 201–224. <https://doi.org/10.1016/j.accfor.2015.05.002>
- 26) Organization for Economic Co-operation and Development. (2023). *G20/OECD principles of corporate governance 2023*. OECD Publishing. <https://doi.org/10.1787/ed750b30-en>
- 27) Power, M. (1997). *The audit society: Rituals of verification*. Oxford University Press.
- 28) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119/1 (2016).
- 29) Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3), 1–28.
- 30) Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).
- 31) Schwab, K. (2016). *The fourth industrial revolution*. Crown Business.

- 32) Sutherland, E. H. (1949). *White collar crime*. Dryden Press.
- 33) Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.