Forensic Secretarial Audit: When Compliance Becomes Detection

Secretarial Audit under Section 204 of the Companies Act, 2013, as currently practised in most boardrooms, is a compliance verification exercise — a structured confirmation that filings were made, registers were maintained, and disclosures were issued within prescribed periods. This article argues that this formulation is insufficient. In an era of structured financial fraud, AI-assisted record manipulation, and deepening regulatory complexity, the secretarial auditor is frequently the first professional to encounter fraud signatures — but is operationally and intellectually unprepared to read them. Drawing on publicly known enforcement actions, regulatory frameworks from India, the UK, and Japan, and the specific governance failures in RBI-regulated NBFCs, this article proposes a forensic methodology for secretarial audit — one grounded in Fraud Risk Assessment, Key Risk Indicators, and intentionality analysis — and addresses the responsibilities of both the practising CS conducting the audit and the in-house CS who must build the internal architecture to make forensic audit possible, rather than adversarial.

CS Raman Narasimhan, FCS
Managing Principal, Mekiki Partners
Chennai
nramans@gmail.com

INTRODUCTION

THE GAP BETWEEN CERTIFICATION AND DETECTION

Every year, thousands of Form MR-3/Secretarial Audit Reports are filed across India's listed and prescribed unlisted company universe. Every year, Secretarial Auditors certify compliance with the Companies Act, SEBI Listing Obligations, FEMA, the Depositories Act, and a growing list of allied statutes. And every year, enforcement actions by SEBI and the MCA reveal fraud signatures — forged board resolutions, backdated filings, related-party transactions structured to obscure beneficial ownership, and statutory delays that were not accidental — that the secretarial audit, conducted weeks or months earlier, did not detect.

This is not an indictment of individual professionals. It is a structural observation about how the secretarial audit function has been designed, executed, and understood. The Form MR-3 format, and the professional culture around it, is inherently backward-looking and binary: was a form filed? Was it filed on time? Was a meeting held? Were registers maintained? What it does not ask — and what no guidance note, checklist, or compliance software currently demands — is the forensic question: *was the record accurate, was the process genuine, and was any deviation from compliance intentional?*

This article argues that the answer to that gap is not merely process improvement. It is a fundamental reconception of what secretarial audit is for. The forensic dimension of secretarial audit — its capacity to detect, not merely certify — must be built into the methodology, not left to chance. And for that to happen, both the practising CS conducting the audit and the in-house CS whose work is being audited must be prepared, motivated, and equipped in ways that current professional standards do not demand of either.

The stakes of this reconception are high. A qualified Form MR-3 with adverse remarks is a governance failure for all parties: it signals that the internal secretarial function was unable to maintain forensic-quality records, that the board either could not or did not act on leading risk signals, and that the auditor arrived to find the damage rather than prevent it. The goal of this article is to show how that outcome can be avoided — and how, done well, forensic secretarial audit becomes the board's most reliable early warning system.

WHAT IS FORENSIC SECRETARIAL AUDIT — AND WHEN DOES IT APPLY?

a. The Legal Boundary

Section 204 of the Companies Act, 2013 mandates secretarial audit for prescribed classes of companies, with the report in Form MR-3 covering compliance with the Companies Act, the Securities Contracts (Regulation) Act, the Depositories Act, FEMA, SEBI regulations, and all sector-specific laws applicable to the company. The statute does not use the word "forensic." It does not require the auditor to assess intent, evaluate risk intelligence, or conduct a fraud risk assessment.

The forensic dimension arises directly from statute. Section 143(14) of the Companies Act, read with Rule 13(5) of the Companies (Audit and Auditors) Rules, 2014, explicitly extends the fraud reporting obligation under Section 143(12) *mutatis mutandis* to the Company Secretary in practice conducting secretarial audit under Section 204. This means the secretarial auditor who has reason to believe that an offence involving fraud is being or has been committed is required to report the matter to the Board or Audit Committee within the prescribed timelines, and thereafter to the Central Government where applicable. Non-compliance attracts a penalty of Rs.5 lakh in the case of a listed company. The secretarial auditor who encounters indicators of intentional non-compliance, record manipulation, or governance evasion and notes it merely as a "delay" or a "lapse" is not just professionally deficient — they are potentially in breach of an explicit statutory obligation.

b. When Does Forensic Audit Apply?

A forensic secretarial audit is triggered, or should be, in at least four circumstances beyond the routine annual appointment:

- A whistleblower complaint involving governance records, Board authorisations, or share register integrity.
- A SEBI or MCA investigation, inspection notice, or adjudication proceeding that requires the secretarial auditor to provide documentation or testify on the company's compliance record.
- An insolvency or restructuring proceeding in which the veracity of board resolutions, related-party authorisations, and statutory filings is directly material to creditor claims or liquidation proceedings.
- A Board-directed special audit following a change in control, a whistleblower disclosure, or a material corporate event whose governance trail is disputed.

But the more important — and more neglected — application of forensic thinking is in the *routine annual audit itself.* Every secretarial auditor who approaches the Form MR-3 as a checklist is leaving forensic value on the table. The question is not whether the environment calls for a special investigation. The question is whether the auditor is trained and prepared to read the compliance record as a risk document, not merely a filing calendar.

> The central argument of this article resolves to a single proposition: the Company Secretary — both as secretarial auditor and as in-house governance professional — is uniquely positioned to perform a forensic function that no other professional in the governance ecosystem currently performs.

THE FRAUD TYPOLOGY: WHAT THE SECRETARIAL AUDITOR ACTUALLY ENCOUNTERS

a. The Mens Rea Problem: Intentional Delay vs. Casual Lapse

The most consequential — and least examined — forensic question in secretarial audit is this: when a statutory filing is late, was it late by accident or by design?

Current Secretarial Audit practice treats every delay identically: it is noted, the penalty paid is recorded, and the report moves on. This is forensically illiterate. A delay in filing Form MGT-14 for a Board resolution approving a related-party transaction — particularly when that delay coincides with a period during which promoters were active in the market — is not the same as a delay in filing an annual return due to administrative overload. The former may constitute evidence of deliberate information withholding to protect insider trading or to defer market reaction to a material corporate decision. The *mens rea* — the intent behind the act — is entirely different, and the consequences for investors are proportionally more serious.

The IndusInd Bank case (SEBI ex-parte interim order, May 2025) illustrates this with precision. SEBI found that material information about the bank's derivative portfolio losses — internally quantified at Rs.1,572 crore as early as December 2023 — was not classified as UPSI until March 4, 2025, and not disclosed to exchanges until March 10, 2025. In the interval of over fifteen months, five senior executives including former MD & CEO Sumant Kathpalia sold substantial shareholdings, avoiding losses of approximately Rs.19.78 crore in aggregate. The secretarial compliance record for that period would have shown disclosure filings within prescribed timelines for most obligations. But a forensic lens — one that cross-referenced the disclosure pattern against the internal communication record and the executive trading pattern — would have identified the gap between *what was known* and *what was disclosed,* and when.

For the practising CS, the implication is direct: every material delay must be interrogated, not just noted. What was in the resolution or disclosure that was filed late? Who benefited from the timing? Was the delay approved at an appropriate level, and was the approval itself documented? For the in-house CS, the implication is equally direct: a culture in which delays are treated as administrative matters rather than governance events is a culture in which the secretarial function cannot provide forensic assurance to the board.

b. Forged and Backdated Board Resolutions

The integrity of the Board resolution is the foundation of the secretarial record. Every subsequent filing, disclosure, approval, and transaction depends on the validity of the board's documented decision. Yet the secretarial auditor, in routine practice, verifies that a resolution exists — not that it is genuine, not that the directors it records as present were actually present, and not that the date it bears reflects when the decision was actually made.

For the secretarial auditor, the governance record of a preferential allotment is directly within scope — the EGM notice, the board resolutions authorising the allotment, and the post-allotment utilisation disclosures under Regulation 32 of LODR (formerly Clause 43 of the Listing Agreement). A forensic secretarial auditor examining the quarterly utilisation filings would have identified, at the very first reporting cycle, that the stated objects and actual application of funds did not match. The pattern, escalated early, would have created an obligation to act — not to wait for SEBI to reconstruct the record years later. Separately, on the resolution integrity question, a forensic secretarial auditor should examine whether board papers, minutes, and attendance registers are internally consistent in chronology and cross-references — and whether the content of resolutions is consistent with disclosures or announcements made proximate to the claimed meeting date.

c. Share Register Manipulation and Fictitious Transfers

The forensic secretarial auditor examining a company's share register must approach it not as a static document to be ticked but as a live record whose integrity is evidence of governance quality. Reconciliation between the register of members, the depository records, and the shareholding patterns filed with exchanges — across multiple time points — reveals whether transfers have been properly authorised, whether beneficial ownership has been accurately reflected, and whether any transfers proximate to material corporate events warrant additional scrutiny. DIN and PAN mismatches, directorial changes in the period immediately before a significant transaction, and unusual clustering of transfers in short windows are all KRI signals that the current MR-3 format neither prompts nor captures.

d. Related-Party Transactions Structured to Obscure Beneficial Ownership

Related-party transactions represent perhaps the highest-risk area in the secretarial record, because the secretarial auditor is uniquely positioned — between the Companies Act register and the board resolution — to identify when the governance architecture of a transaction has been constructed to avoid the appearance of a related-party relationship while preserving its economic substance.

A forensic secretarial auditor examining related-party transactions must cross-reference the register of directors, the beneficial ownership declarations under Section 89/90, and any prior disclosures of interest under Section 184, against the counterparties to every material transaction. Where a transaction's counterparty appears unrelated on the face of the register but shares a beneficial owner, a common address, a DIN-linked directorship, or a common professional adviser with the company or its promoters, the auditor has a forensic obligation to flag the pattern — not to adjudicate the relationship, but to require management to produce the documentary basis for the related-party determination.

DETECTION TOOLS: FROM FILING CALENDARS TO FORENSIC METHODOLOGY

a. The Fraud Risk Assessment as the Starting Point

The most significant structural reform proposed in this article is this: **the secretarial audit must begin with a Fraud Risk Assessment, not a filing calendar.** This is not current practice anywhere in India. But it is the only logical starting point for an audit that aspires to forensic quality.

A Fraud Risk Assessment (FRA) in the secretarial context maps the areas of greatest vulnerability to intentional non-compliance or record manipulation in the specific company being audited. It is not a generic checklist. It is calibrated to the company's size, sector, ownership structure, recent corporate history, and regulatory exposure. For a promoter-dominated listed company, the FRA would weight the integrity of related-party authorisations and the consistency of insider trading declarations heavily. For a company that has recently undergone a change in control or a major restructuring, it would weight the validity of board resolutions and the accuracy of the register of members.

The FRA produces the secretarial auditor's *risk-rated work plan* — a prioritisation of where forensic attention is warranted, not a mechanical enumeration of what forms were filed. Without the FRA, the audit is process-driven. With it, the audit is risk-driven — which is what "forensic" means in practice.

For the in-house CS, the FRA creates a corresponding obligation: the company should itself maintain a Compliance Risk Matrix — updated at least annually and reviewed whenever a material corporate event occurs — that documents the identified compliance risks, the controls in place, and the residual risk position. This is the document the forensic secretarial auditor should be given on Day 1 of the audit, not constructed from scratch by the auditor at the client's premises.

b. Key Risk Indicators: Leading, Lagging, and Tier 1

Compliance management tools currently available in the Indian market offer what may be called "traffic light compliance" — colour-coded dashboards showing filed/overdue/at-risk status across a filing calendar. These tools have genuine utility for operational compliance management. They have no forensic utility. They tell the auditor what was filed. They do not tell the auditor *why* something was filed late, *whether* the content filed was accurate, or *what the pattern* of filings reveals about governance quality over time.

A forensic secretarial audit requires Key Risk Indicators — a concept well-established in financial risk management but entirely absent from secretarial audit practice. In the secretarial context, KRIs fall into three tiers:

Leading KRIs — signals that precede governance failure:

- Frequency of board meeting adjournments or quorum failures in a rolling 12-month window.
- Number of resolutions passed by circulation versus in meeting — and whether the topics passed by circulation were material.
- Pattern of related-party transaction approvals — whether they cluster around specific reporting periods.
- Frequency of Section 184 declarations being filed after the related event rather than before.
- Directorial changes in the 60-day period proximate to a material announcement or transaction.

Lagging KRIs — patterns revealed by historical compliance data:

- Rolling late filing frequency by category and by individual responsible — distinguishing systemic overload from selective delay.
- Penalty payment history — does the company pay penalties promptly (suggesting administrative lapse) or contest them (suggesting strategic non-compliance).
- Qualified MR-3 observations that recur across consecutive audit periods without remediation.

Tier 1 KRIs — high-consequence signals requiring immediate escalation:

- Beneficial ownership changes (Section 89/90 declarations) proximate to open-offer thresholds.
- UPSI designation gaps — periods during which material information was known internally but not designated as UPSI and not reflected in trading window closures.
- Register of directors disclosing a DIN flagged in MCA21 enforcement records.

None of these KRIs require the secretarial auditor to make a legal determination. They require the auditor to *ask the question* — and to document, in the working papers, both the question asked and the answer received. That documentation is itself forensic evidence of the audit's quality.

c. Blind Spot Reviews: What the Auditor Was Not Shown

A process audit asks: did the process work? A forensic audit asks: was the process designed to obscure? The practical expression of this distinction is the blind spot review — a structured examination of *what the auditor was not shown,* rather than what was produced.

Blind spots in secretarial audit typically include: board papers that were circulated informally and not retained in the official file; draft minutes that differ from the signed minutes; digital signature logs that do not match the dates on signed documents; and statutory register entries that are complete in the copy provided to the auditor but incomplete in the original or in a different version held by a different function. A forensic secretarial auditor must routinely request the *source* documents — not the copies prepared for the audit — and must cross-reference digital metadata (creation dates, modification dates, author fields) against the dates on the face of the document.

This is where the DPDPA dimension enters naturally. When the forensic secretarial auditor accesses personal data in the course of the audit — Director Identification Numbers, shareholder PAN records, beneficial ownership declarations, or electronic signature metadata — they are accessing data within the meaning of the Digital Personal Data Protection Act, 2023. The audit engagement letter must address the data fiduciary obligations created by this access: the basis on which personal data is being processed (legitimate use under the Companies Act and SEBI regulations), the retention and deletion protocols for data accessed during the audit, and the prohibition on using personal data accessed in the audit engagement for any other purpose. AI-assisted tools that cross-reference MCA21 data, depository records, and exchange filings — increasingly used by larger secretarial audit firms — must be configured to ensure that the personal data accessed through these tools is processed in compliance with the DPDPA's data minimisation and purpose limitation principles. The in-house CS, as the entity whose data is being accessed, should ensure that the company's data processing register reflects the secretarial audit engagement as a legitimate processing activity.

d. Global Reference Points: What Other Jurisdictions Demand

India's secretarial audit has no precise equivalent in most developed governance jurisdictions — which makes it, in principle, one of the most powerful

governance tools available to Indian boards. The challenge is that it has been executed at the lowest level of its potential.

In **Japan**, the Financial Instruments and Exchange Act (FIEA, 2006 — commonly referred to as J-SOX) requires listed companies to conduct and certify internal control assessments over financial reporting, with those assessments attested by the same external auditor who signs the financial statements. Crucially, J-SOX mandates *risk assessment as the foundation* of the internal control evaluation — management must identify key controls, assess their design and operating effectiveness, and the auditor must evaluate the risk-based work plan, not merely the output. This is the structural equivalent of what we are proposing for Indian secretarial audit: the audit begins with risk, not with a calendar.

In the **United Kingdom**, the revised UK Corporate Governance Code (2024) introduced Provision 29, which for the first time requires boards to make a formal declaration on the effectiveness of their *material* internal controls — explicitly including controls over fraud and override of controls. The company secretary in a UK-listed company is directly responsible for ensuring that the board's internal control framework is documented, reviewed, and accurately described in the annual report. This places the UK company secretary in precisely the forensic posture we are advocating here: responsible not merely for compliance procedures but for the *integrity* of the controls that those procedures are meant to enforce.

The lesson for Indian practice is not that we must replicate these frameworks wholesale. It is that the instinct behind them — that governance audit must be risk-based, that the auditor's starting point is *where are the vulnerabilities* rather than *what are the obligations* — is a professional standard that Indian secretarial audit can and must adopt.

PROFESSIONAL LIABILITY AND REPORTING OBLIGATIONS WHEN FRAUD IS DETECTED

a. The Legal Framework

When a secretarial auditor encounters material indicators of fraud — not conclusive proof, but substantiated indicators — the legal and professional obligation is clear, though frequently misunderstood in practice. Contrary to common assumption, Section 143(12) of the Companies Act — the fraud reporting obligation — is not limited to statutory auditors. Section 143(14), read with Rule 13(5) of the Companies (Audit and Auditors) Rules, 2014, explicitly applies the provision *mutatis mutandis* to the Company Secretary in practice conducting secretarial audit under Section 204. The secretarial auditor therefore operates under the same framework as the statutory auditor in this respect:

- Section 143(12) read with Rule 13(5): where the secretarial auditor has reason to believe that a fraud is being or has been committed against the company by its officers or employees, the matter must be reported to the Board or Audit Committee within the prescribed timelines, and thereafter to the Central Government where applicable. Failure to comply attracts a penalty of Rs.5 lakh (listed companies).
- Section 204(4), which requires the Board to explain in full any qualification or observation in the MR-3 — making the qualified report itself a board-level accountability document.
- The ICSI Code of Conduct, which requires members to act in the public interest and to report matters of significance through appropriate channels.
- SEBI LODR Regulation 24A and related provisions, which create obligations around material compliance failures affecting investor protection.
- The PMLA, 2002, whose applicability to Company Secretaries in practice has expanded as the Enforcement Directorate has pursued secretarial record chains in money laundering investigations.

In practical terms, the secretarial auditor who identifies what appears to be a pattern of intentional non-compliance has three escalation pathways: a qualified Form MR-3 that documents the specific finding and its basis; a direct communication to the audit committee (not to management, whose integrity may be in question) citing the specific indicators and requesting an explanation; and, in cases involving potential market abuse or investor harm, a report to SEBI under the relevant regulations. The choice between these pathways depends on the severity of the indicator, the company's response to audit queries, and the professional judgement of the auditor — but the framework for that choice must be pre-determined, not improvised at the point of discovery.

b. The Qualified Report: Not the End, but the Beginning

A qualified Form MR-3 is frequently treated by both auditors and companies as the worst outcome of the audit — a reputational penalty to be avoided through negotiation and remediation. This framing is backwards. A qualified report that is specific, evidence-based, and graduated in its assessment of severity is a *forensic document of value* — to the board, to the audit committee, to future auditors, and to regulators. The secretarial auditor who produces a generic qualification ("the company has not complied with Regulation X in respect of Y filings") is providing less forensic value than one who documents the specific indicators, the queries raised, the responses received, and the basis for the conclusion that the lapse was either inadvertent or systemic.

For the in-house CS, the critical implication is this: a qualified report is far less damaging to the company, and to the in-house CS personally, if it is anticipated, documented, and presented to the board with a remediation plan before the MR-3 is finalised. The in-house CS who waits for the auditor to discover a compliance failure and qualify the report has lost the initiative. The in-house CS who identifies the failure first, reports it to the audit committee, and works with the secretarial auditor to document the finding and the remediation has demonstrated exactly the governance function that the board expects and that the audit was designed to provide.

THE NBFC GOVERNANCE FAILURE: DUAL HATTING AND THE LIMITS OF CHECKLIST COMPLIANCE

No area of current secretarial audit practice better illustrates the gap between compliance certification and forensic detection than the treatment of dual-hatting in RBI-regulated entities — and specifically the practice, common in smaller and mid-tier NBFCs, of the Company Secretary simultaneously holding the designation of Chief Compliance Officer.

The RBI's April 2022 Circular on Compliance Function and Role of Chief Compliance Officer for NBFCs was explicit on this point. The CCO, it stated, must be a senior executive not below two levels from the CEO, must possess domain expertise in risk management and regulatory compliance, must have independent reporting lines to the MD/CEO or the Risk Management Committee of the board, and — critically — *"there shall not be any dual hatting, i.e., the CCO shall not be given any responsibility which brings elements of conflict of interest."*

The RBI's concern is not procedural. It is structural. The CCO's role in an NBFC encompasses compliance with RBI's prudential norms, KYC/AML obligations, Fair Practices Code requirements, interest rate transparency obligations, and a growing body of conduct regulation that has no connection to company law or SEBI regulations. A Company Secretary trained in MCA filings, SEBI LODR compliance, and secretarial practice is not — by training, by certification, or by professional formation — equipped to assess compliance risk in these domains. Assigning the CCO designation to the CS is a cost-saving measure that creates a *compliance fiction:* the form of compliance oversight without its substance.

For the secretarial auditor of such an NBFC, this creates a direct forensic challenge. The MR-3 covers compliance with applicable laws — but how does the auditor certify compliance with RBI's operational compliance framework when the person responsible for that compliance has neither the training to discharge it nor the independence to report failures upward? The honest answer is that in the current practice, the auditor does not examine it. The CCO designation is noted; the existence of a Board-approved Compliance Policy is verified; and the audit moves on.

A forensic approach would require the auditor to assess: whether the CCO (i.e., the CS) has actually conducted the annual Compliance Risk Assessment mandated by the RBI Circular; whether the compliance function's findings have been independently reported to the Board or Board Committee; whether any material compliance failures identified by the RBI in its own inspections have been escalated to the audit committee with a root-cause analysis; and whether the dual-hatting itself has been disclosed to the board as a structural governance risk. Identifying dual-hatting and its limitations is not a criticism of the individual CS holding both roles — it is a forensic observation that the board must be made aware of, because it is the board that bears responsibility for the adequacy of its governance architecture.

THE COMPANY SECRETARY AS THE PROFESSION'S FORENSIC SENTINEL

The central argument of this article resolves to a single proposition: the Company Secretary — both as secretarial auditor and as in-house governance professional — is uniquely positioned to perform a forensic function that no other professional in the governance ecosystem currently performs.

The statutory auditor examines financial records. The internal auditor examines process effectiveness. The Risk Management Committee examines strategic and operational risk. The Audit Committee oversees all of these. But none of these functions examines the *statutory and governance record* with the combination of legal knowledge, board proximity, and regulatory breadth that the Company Secretary brings. The statutory registers, the board resolution file, the insider trading compliance records, the beneficial ownership declarations, the LODR disclosure calendar — these are the CS's domain, and their integrity is the CS's professional responsibility.

What this article has proposed is that the profession operationalise that responsibility through a forensic methodology: begin every secretarial audit with a Fraud Risk Assessment; read every compliance deviation through the lens of intent, not merely outcome; deploy Key Risk Indicators to identify patterns that a filing calendar cannot reveal; conduct blind spot reviews of what was not produced; and approach the qualification of the MR-3 as a forensic document rather than a reputational penalty.

For the in-house CS, the corresponding obligation is to build the internal architecture that makes forensic audit possible. That means maintaining a Compliance Risk Matrix that is updated proactively rather than retrospectively; treating every delay, deviation, or qualification as a governance event requiring root-cause analysis; ensuring that the board understands the difference between a checklist compliance function and a risk-intelligent governance function; and having the professional confidence to bring emerging forensic concerns to the audit committee before they become qualified report observations.

ICSI's evolving curriculum and its engagement with AI governance, digital compliance tools, and DPDPA

frameworks reflect an institutional recognition that the governance landscape has shifted in ways that the profession must keep pace with. The forensic dimension of secretarial audit is the next frontier of that evolution — and it is one that Company Secretaries are, by their statutory position and professional formation, uniquely equipped to lead.

CONCLUSION

Secretarial Audit has the potential to be India's most powerful routine governance tool. The Company Secretary who signs the Form MR-3 sits at the intersection of the board's decision record, the company's statutory obligations, and the regulator's disclosure expectations. No other professional occupies that position with that breadth of access and that depth of governance responsibility.

The profession has not yet realised that potential, because it has allowed secretarial audit to become synonymous with filing verification. The forensic dimension — the capacity to detect intentional non-compliance, to read compliance patterns as risk signals, to identify the governance architecture of fraud before it becomes the subject of an enforcement order — has been left, by default, to SEBI investigators and forensic accountants who arrive after the event.

The time to reclaim that ground is now. The regulatory environment — SEBI's expanding enforcement reach, the RBI's explicit CCO independence requirements, the UK's Provision 29 internal controls declaration, and Japan's risk-based J-SOX framework — is converging on a governance standard that treats the audit of governance records as a risk function, not a compliance function. India's secretarial audit, with its statutory basis and its direct board access, is structurally better positioned than most equivalent mechanisms globally to meet that standard.

The Company Secretary who walks into a secretarial audit with a Fraud Risk Assessment in hand, who asks the forensic questions about every material delay, who cross-references the board resolution against the trading record, who flags the dual-hatting governance failure to the audit committee, and who qualifies the Form MR-3 with specificity and evidence when the situation demands it — that professional is not performing a support function. They are performing a leadership function. That is the standard the profession must set for itself.

REFERENCES:

i. *Companies (Audit and Auditors) Rules, 2014 — Rule 13(5): explicit extension of fraud reporting obligation to Cost Auditors and Secretarial Auditors.*

ii. *Companies Act, 2013 — Section 204 (Secretarial Audit), Section 143(12), (14) (Fraud reporting obligation, extended mutatis mutandis to secretarial auditors), Section 184/188/89/90 (related-party and beneficial ownership disclosures).*

iii. *Financial Reporting Council (FRC). (2024). UK Corporate Governance Code 2024 — Provision 29: Material Internal Controls Declaration. FRC, London.*

iv. *Financial Services Agency, Japan. (2007). Standards for Management Assessment and Audit Concerning Internal Control over Financial Reporting (J-SOX). Business Accounting Council, FSA Japan.*

v. *Institute of Company Secretaries of India (ICSI). Guidance Note on Secretarial Audit. ICSI.*

vi. *Ministry of Electronics and Information Technology (MeitY). (2023). Digital Personal Data Protection Act, 2023. Government of India.*

vii. *Prevention of Money Laundering Act, 2002, as amended — applicability to governance professionals in secretarial audit contexts.*

viii. *Reserve Bank of India. (2022). Compliance Function and Role of Chief Compliance Officer (CCO) — NBFCs. RBI Circular, April 11, 2022.*

ix. *Reserve Bank of India. (2024). Internal Compliance Monitoring: Single Dashboard Circular for Banks and NBFCs. RBI/2023-24/117, January 31, 2024.*

x. *SEBI Adjudication Order — Cameo Corporate Services Ltd. — forged banker attestations, duplicate share issuance, improper transfer rectifications. SEBI.*

xi. *SEBI. (2015). SEBI (Prohibition of Insider Trading) Regulations, 2015, as amended.*

xii. *SEBI. (2021). SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 — Amendment, 2021.*

xiii. *Securities and Exchange Board of India (SEBI). (2025). Ex-parte Interim Order in the matter of IndusInd Bank Limited — insider trading and delayed UPSI disclosure (WTM/KCV/IVD/SEB/04/2025-26, May 28, 2025). SEBI Enforcement.*

xiv. *Supreme Court of India. (2026). Securities and Exchange Board of India v. Terrascope Ventures Ltd. & Ors., 2026 INSC 245, 2026 SCC OnLine SC 403, decided 17-3-2026 — diversion of preferential allotment proceeds; shareholder ratification incapable of curing fraud under PFUTP Regulations.*