

FORENSIC FORESIGHT MONTHLY

Issue 01



June 2026

Financial Crime · Forensic Accounting · Investigation

by Dr. (CA) Durgesh Pandey

WHAT'S INSIDE THIS ISSUE?

- The Moment a Forensic Report Leaves The Room
- Favouring The Vendor: A Hospital Procurement Investigation
- The Fraudster Has Entered The System

A WORD ON TERMINOLOGY, BEFORE WE BEGIN

EDITORIAL NOTE

The term forensic audit appears widely in practice in the Indian context, in bank communications, court orders, regulatory instructions, and even in the Supreme Court judgment discussed in this issue. We have reproduced that language where it appears in source material. However, the Institute of Chartered Accountants of India, through its Forensic Accounting and Investigation Standards (FAIS), has explicitly advised against the use of the term forensic audit. The correct and professionally recognised term is Forensic Accounting and Investigation (FAI). This distinction is not semantic.

Forensic accounting and investigation is a discipline that encompasses financial analysis, evidence evaluation, fraud examination, and litigation support. Describing it as an audit misrepresents its scope and the nature of the practitioner's responsibilities.

Forensic Foresight Monthly will follow FAIS terminology in its own analysis and commentary. Where forensic audit appears in quoted material or case citations, it is reproduced as used in the original source. For practitioners at the start of their careers, vocabulary is not a formality. Use the right term from the beginning.



THE MOMENT A FORENSIC REPORT LEAVES THE ROOM

THE FORENSIC BRIEF

Why the Supreme Court's latest ruling on bank fraud classification makes report quality harder to ignore

When a forensic audit report moves beyond the bank's file

In *State Bank of India v. Amit Iron Private Limited & Ors.*, decided on 7 April 2026, the Supreme Court clarified that a borrower does not have an automatic right to a personal hearing before fraud classification. But where the bank considers audit reports, including forensic audit reports, those reports must be furnished to the borrower before the final decision is taken. For forensic professionals, this is the point to note: a report prepared for a bank may not remain an internal document. Once it supports a fraud classification, it becomes part of the decision-making record and must be capable of being read, questioned, and understood outside the engagement.

Can the report explain its own conclusion?

A report that was earlier read only by the bank may now be examined by the borrower, lawyers, regulators, investigators, and courts. The important shift is not only that the borrower may receive a copy of the forensic audit report. The real issue is what happens when the report is read by someone outside the original engagement.



1. The finding must show its path

A forensic report should not merely state that funds were diverted, stock was inflated, or transactions were suspicious.

It should show the trail:

- what was examined,
- what was found,
- what explanation was tested, and
- why the conclusion follows from the evidence.

2. The language must match the evidence

There is a difference between a red flag, an irregularity, suspected diversion, and an established finding. If the evidence supports only a concern, the report should not use language that sounds like a final fraud conclusion.

3. The limitations must be visible

A good report does not hide what could not be verified. If third-party confirmations were not received, system access was limited, records were incomplete, or management explanations could not be independently tested, the report should say so clearly.

4. The report should not depend on oral explanation

The investigator may not be present when the report is later challenged. The document should carry enough reasoning for an external reader to understand how the conclusion was reached.

What to carry forward from this

- A forensic audit report may not remain an internal bank document if it is relied upon for fraud classification.
- The report must show the path from red flag to finding.
- Strong conclusions need visible reasoning and supporting evidence.
- The language of the report should match the strength of evidence.
- Limitations, assumptions, and unresolved gaps should be clearly stated.
- A report prepared for one reader may later be tested by many readers.

FAVOURING THE VENDOR: A HOSPITAL PROCUREMENT INVESTIGATION

CASE IN THE DOCK

As per ACFE’s RTTN, tips are the single most common fraud detection method globally. But not every fraud investigation begins with a whistleblower tip or a regulator’s knock. Sometimes it begins with a new management team asking a simple question: Were procurement decisions made on merit, or on something else?

In this case, the answer took three years of records and a field verification of vendor offices to establish.

How a procurement review moved from policy testing to a Rs. 12 crore fraud finding.

A large tertiary care hospital had received government funding of more than Rs. 200 crore. After a change in management, the new leadership called for a forensic review of procurement activity over the previous three years.

The concern was direct: had the procurement process been manipulated to favour selected vendors?

The team began with that working hypothesis. Based on value and risk, the review covered items that formed nearly 20% of procurement volume but 80% of procurement value. Every contract and transaction within the selected range was then examined.

ORGANISATION	Large tertiary care hospital
TRIGGER	Change in management; review of three years of procurement
ISSUE UNDER REVIEW	Whether procurement was shaped to favour selected vendors
FINDING	Fraud quantified at Rs. 12 crore
ACTION TAKEN	Employees placed on compulsory leave; complaint filed; vendors blacklisted; procurement policy revised

How the review was structured

The policy came first

The team first reviewed the hospital’s procurement policy. This gave the investigators the benchmark against which every tender, RFQ, approval, and vendor selection could be tested. Records of RFQs and tenders were called for. Tender minutes, bidder restriction criteria, bid evaluation sheets, L1 and L2 comparisons, approval notes, and award decisions were examined.

The review focused on signs of process manipulation, including:

- tailoring of bid specifications
- dilution of tender conditions
- restricted competition
- unusual timing patterns
- confidentiality breaches
- repeated awards to the same vendors
- unexplained differences between L1 and L2 quotations

From this review, high-risk vendors were selected for deeper examination.

What made the vendors stand out

Some red flags sit outside the invoice

The vendor review went beyond purchase files and payment records. The team checked when each vendor was incorporated, how much of its business came from the hospital, whether it had other customers, and whether its office premises matched the scale of work awarded.

Field visits were also carried out. But then a few facts stood out. Several vendor companies had been incorporated close to the dates of the tenders they later won. At least one vendor appeared to have the hospital as its only buyer. Some companies were operating from home offices that did not support the volume of business shown in the hospital records.

The team also cross-checked vendor addresses with employee addresses and made open-market enquiries for similar products from alternative suppliers.

The employee link

Vendor favouritism usually needs someone inside the system

The investigation then moved to internal controls within the procurement function. Segregation of duties was tested. The roles of procurement officers, approval authorities, and bid evaluation members were reviewed. The team also examined the relationship between employees and vendors, especially around L1 and L2 bidders.

Where relevant, the behavioural profile, social proximity, and lifestyle of key employees were verified. These indicators were treated with care. A lavish lifestyle or a close relationship does not prove fraud on its own. But when it appears alongside tender manipulation, vendor concentration, and weak controls, it becomes important corroborative material.

What the investigation found

The pattern was wider than one weak tender

The review found that favour had been extended to selected vendors. One vendor company was directly connected to a hospital employee, although the employee was not working in the procurement department. Several vendor entities had been incorporated around the time of the tenders awarded to them. At least one vendor had no meaningful customer base outside the hospital.

The physical presence of some vendors also raised concerns. Their offices did not justify the size and volume of business recorded with the hospital. The investigation further identified a lavish lifestyle of a relevant employee and an unusually close vendor-employee relationship.

The quantified fraud was established at Rs. 12 crore.

Outcome

The findings led to immediate action

The hospital placed employees on compulsory leave pending enquiry. A complaint was filed with law enforcement. The identified vendors were blacklisted. A stricter procurement policy was also introduced.

The case showed how procurement fraud often takes shape much before the invoice is raised. The favour may begin with specifications, bidder eligibility, restricted competition, evaluation decisions, or approvals.



What this case teaches

- A procurement fraud review should begin with the policy. The rulebook gives the investigator the benchmark.
- Vendor incorporation date is a simple but powerful red flag, especially when it falls close to the tender date.
- A vendor with the hospital as its only major customer deserves closer scrutiny.
- Field verification matters. Vendor office size, location, and activity can reveal whether the business volume is realistic.
- Lifestyle and social profile checks can support the investigation when they are linked to transaction findings.
- Segregation of duties failure is more than a control weakness. In procurement fraud, it can become the route through which favour is operationalised.

KNOW THE TERM

Hypothesis

A testable foundation for the investigation

The word hypothesis comes from the Greek idea of something “placed under” an argument, as the foundation on which reasoning is built. In forensic work, it is not a guess and it is not a softened way of stating a conclusion. It is a proposition that guides the investigation and remains open to being proved wrong. The ACFE approach to fraud examination also follows this discipline through theory development and testing, where the examiner forms a possible explanation, looks for evidence that supports or contradicts it, and modifies the direction as facts emerge. ICAI’s FAIS 140 on Applying Hypotheses brings the same idea into forensic practice by requiring hypotheses to be developed, tested, revised where necessary, and linked to the scope and objectives of the assignment.

In the hospital procurement case discussed in this issue, a weak starting point would be: “The vendor was favoured.” It sounds direct, but it already assumes the answer. A better forensic hypothesis would be: “Procurement decisions may have been influenced by an undisclosed employee-vendor relationship, resulting in award of contracts that did not follow the hospital’s procurement policy.” This gives the team something specific to test through tender records, vendor profiles, employee links, approval notes, price comparisons, and policy compliance. A good hypothesis does not push the investigation toward a preferred finding. It should aim to give the investigation a disciplined path.

Practical test: Before starting, ask: If this hypothesis is wrong, what evidence would show that?

PRACTITIONER'S PERSPECTIVE

The Fraudster Has Entered the System

A reflection from DxFS 2026 on
why digital fraud is no longer
an outsider problem

At the DxFS 2026 summit in Hyderabad, hosted by DAAB ICAI, the panel discussions and my conversations with fellow professionals pointed to the same concern: fraud is no longer waiting outside the organisation.

For years, digital fraud was spoken about as an external attack. Someone hacked into a system. Someone sent a phishing link. Someone impersonated an officer, a banker, or a customer. That risk still exists. But the more difficult frauds today are not always outside the gate but now inside trusted processes, approved workflows, boardroom decisions, vendor systems, customer journeys, and digital evidence trails.

The uncomfortable part is that AI-enabled fraud does not always look like a breach. It may come through a familiar face on a video call, a cloned voice giving urgent instructions, a synthetic document that looks procedurally correct, or a vendor profile that appears complete in the system. The customer may authorise the transfer. The employee may approve the transaction. The control may record that the process was followed. That is why the practitioner's work has to move beyond checking whether the transaction was valid on paper.

The harder question is whether the belief behind the transaction was manipulated.



Document testing

Was the document genuine?

→ Was the situation manufactured?

Approval testing

Who approved the transaction?

→ What made them believe the approval was valid?

Control testing

Did the control operate?

→ Was the control looking at the right risk?

That is why AI, digital transformation, fraud response, and FAIS cannot be treated as separate conversations. In practice, they now meet inside the same case file. A digital fraud may begin with impersonation, move through a banking channel, rely on weak controls, create a misleading document trail, and end as a forensic investigation. No single function sees the whole picture by default. Technology teams see the system, while compliance teams see the alert, and business teams see the transaction. Finally, investigators see the trail after damage is done.

The practitioner's role is to connect these fragments early enough for the organisation to act.

That, for me, was the strongest takeaway from DxFS. The profession now needs practitioners who can do more than use tools or quote standards. They must understand how behaviour, systems, evidence, controls, and accountability meet inside a real case.

A QUESTION FOR ISSUE 02

When AI makes a transaction look valid, but the belief behind it was manipulated, where should professional responsibility begin? Is it with the system, the control owner, or the practitioner reviewing the trail?



FORENSIC
FORESIGHT
MONTHLY



Issue 01

June 2026

FINAL FORESIGHT

A forensic finding gains strength when it can travel beyond the investigator, beyond the client, and beyond the first explanation.

Dr. Durgesh Pandey · FCA, CFE, PhD · DKMS & Associates

Forensic Foresight Monthly

#ForensicAccounting #FraudInvestigation #FinancialCrime

#CA #CFE #ICAI

WRITE TO US AT FORENSIC4SIGHT@GMAIL.COM. ONE RESPONSE
WILL APPEAR IN THE NEXT ISSUE WITH EDITORIAL COMMENT.