FROM RED FLAGS TO PREVENTIVE INTELLIGENCE: BUILDING AN INTELLIGENCE-LED FRAMEWORK FOR DETECTING FINANCIAL FRAUD BEFORE INSTITUTIONAL COLLAPSE

Ananya Pillai, B.B.A. LL.B. (Hons.), MIT-WPU School of Law

ABSTRACT

Financial fraud is often treated as an event that becomes visible only after financial loss, regulatory intervention or institutional failure. This approach, however, overlooks the warning signs that frequently precede the fraud. Unusual transactions, accounting irregularities, management override, unexplained relationships with vendors, resistance to audit, excessive concentration of authority and organisational silence may individually appear inconclusive, but their significance changes when they are evaluated collectively. The central argument of this article is that the primary challenge faced by institutions is not necessarily the absence of red flags, but the failure to convert fragmented warning signals into timely and reliable intelligence. Drawing from fraud risk management literature, audit standards, Indian regulatory frameworks and the intelligence analysis principles, this article proposes an intelligence-led framework comprising risk mapping, indicator collection, source evaluation, corroboration, pattern recognition, threat assessment, escalation, preventive intervention and continuous review. The article also looks at the limits of such a framework, particularly the risks of false positives, confirmation bias, reputational harm, excessive surveillance and the improper treatment of suspicion as proof. It argues that preventive intelligence should not replace investigation or legal proof; rather, it should enable institutions to identify where closer scrutiny and preventive action are warranted before fraud develops into institutional collapse.

Keywords: financial fraud, red flags, preventive intelligence, fraud risk management, corporate governance, early warning signals, whistleblowing, institutional risk.

Introduction

Financial fraud rarely begins with the moment at which it is finally discovered. In many cases, the eventual discovery merely represents the point at which previously existing irregularities can no longer be ignored. An unexplained accounting entry, an unusual payment, an overly close relationship with a vendor, repeated management overrides or resistance to an audit query may not, by themselves, establish fraudulent conduct. However, when such indicators accumulate across different parts of an organisation, they may reveal a developing pattern of risk.

This distinction is important because financial fraud is not simply a question of individual dishonesty. It is also an institutional risk. Fraud may be committed by an individual, but it can survive for long periods because of weak controls, inadequate supervision, organisational pressure, conflicts of interest, ineffective audit mechanisms or a culture in which employees are discouraged from questioning senior management. The Association of Certified Fraud Examiners' global research shows the scale and variety of occupational fraud and the importance of examining how fraud is detected within the organisations (ACFE, 2024).

The traditional response to suspected fraud is largely reactive: investigate once an incident has occurred, identify the wrongdoer, quantify the loss and determine legal or disciplinary consequences. Investigation remains necessary, but waiting for sufficient evidence of completed fraud may mean that the institution has already suffered substantial financial and reputational damage. The more useful question, therefore, is whether institutions can act at an earlier stage, when there is suspicion but not yet proof.

This article argues that they can, provided that red flags are not treated as conclusions. A red flag should instead trigger a structured process through which information is collected, its reliability is assessed, related indicators are corroborated, patterns are identified, risk is assessed and appropriate action is escalated. This approach draws from the principles of fraud risk management, intelligence analysis and organisational governance.

The proposed movement is therefore:

Red flag → evaluation → corroboration → pattern → risk assessment → escalation → prevention.

The purpose is not to predict fraud with certainty. It is to improve institutional decision-making before the consequences become irreversible.

Research Question and Aim

The central research question is:

How can institutions convert financial, behavioural, procedural and organisational red flags into a preventive intelligence framework capable of detecting financial fraud before institutional collapse?

The aim is to develop an intelligence-led approach which allows institutions to distinguish isolated anomalies from meaningful patterns of risk, while maintaining the distinction between suspicion, intelligence and legally established proof.

The article addresses three subsidiary questions. First, what types of financial, behavioural and organisational indicators may signal developing fraud risk? Second, how can institutions evaluate and combine such indicators without prematurely treating them as proof of misconduct? Third, what institutional mechanisms are necessary to ensure that credible warning signals result in timely preventive action?

Conceptual Lens: From Fraud Risk Management to Preventive Intelligence

Fraud risk management provides the first ideal foundation for the proposed framework. The COSO–ACFE Fraud Risk Management Guide treats fraud as a risk requiring structured governance, rather than just post-event punishment (COSO & ACFE, 2023). This approach places responsibility on the institution to understand where fraud could occur and establish mechanisms that would identify and respond to them.

The second lens is intelligence analysis. Intelligence is not synonymous with raw information. The intelligence process involves collection, evaluation, analysis and dissemination. An important aspect of this process is evaluating the reliability of both information and its source before drawing conclusions (UNODC, 2011).

This distinction is particularly useful in financial fraud. An anonymous allegation, an unusual transaction identified by software and an auditor's documented observation are all pieces of

information, but they do not necessarily possess the same reliability. Treating them as equally probative may produce either false accusations or missed risks.

The third lens is organisational culture. Fraud cannot be understood entirely through numbers because the environment in which the numbers are produced also matters. Pressure to meet unrealistic targets, excessive concentration of control, fear of questioning senior management, weak whistleblower protection and the normalisation of minor violations can create conditions in which larger misconduct becomes easier to conceal.

These three perspectives are therefore complementary. Fraud risk management provides the institutional structure; intelligence analysis provides the method of evaluating and connecting information; and organisational culture explains why institutions may fail to act even when warning signs exist.

Financial Fraud and the Problem of Fragmented Red Flags

Financial fraud takes several forms, including fraudulent financial reporting, asset misappropriation, corruption, procurement fraud, loan fraud, related-party abuse and concealment through documentation. The specific method may differ, but a common feature is that the conduct often creates inconsistencies that can be observed before the complete scheme is uncovered.

Accounting and financial indicators may include unexplained revenue growth, repeated journal adjustments, delayed reconciliations, unusual transactions, unexplained round-number payments, discrepancies between reported growth and cash flows, vendor concentration and management override of internal controls. Audit standards recognise the importance of professional scepticism precisely because apparently reasonable financial information may contain material misstatements arising from fraud.

However, financial indicators should not be examined in isolation. Behavioural indicators can provide additional context. These may include unusually close relationships with vendors or customers, excessive control over particular processes, reluctance to delegate, defensiveness when questioned, resistance to audit procedures or unexplained lifestyle changes. The ACFE's research on behavioural red flags demonstrates that such indicators recur across occupational fraud cases, although none can independently establish fraudulent conduct (ACFE, 2020).

Organisational indicators may be even less visible. A compliance department that repeatedly remains silent, an audit committee that fails to challenge management, employees who are afraid to report concerns, or an internal process that permits one individual to initiate, approve and record a transaction can reveal structural vulnerabilities.

The problem is therefore not simply that institutions lack information. Information may exist in different places: finance may notice unusual transactions, procurement may notice vendor irregularities, internal audit may notice control failures and employees may notice behavioural changes. If these observations remain within separate institutional compartments, the organisation may possess all the information necessary to identify a developing risk but still fail to see the pattern.

Why Institutions Miss Red Flags

There are several reasons why warning signals fail to produce preventive action.

First, individual anomalies are easy to rationalise. A delayed reconciliation may be attributed to workload. An unusual payment may be explained as a business necessity. A close relationship with a supplier may be considered ordinary. Each explanation may be reasonable when considered independently.

Second, organisations may suffer from information fragmentation. Different departments may possess different pieces of the same developing problem without any mechanism for combining them.

Third, hierarchy can interfere with escalation. Employees may hesitate to report concerns involving senior executives, particularly where the organisation rewards performance aggressively or has weak whistleblower protections.

Fourth, confirmation bias can affect decision-makers. Once management has formed an initial belief that an employee, transaction or department is trustworthy, contradictory information may be discounted. Intelligence analysis literature has long recognised that analysts can unconsciously favour information supporting an existing hypothesis (Heuer, 1999).

Finally, institutions may confuse the absence of proof with the absence of risk. A warning signal does not justify an accusation, but neither should the lack of conclusive proof justify

ignoring the warning. This is the point at which preventive intelligence becomes useful.

From Red Flags to Preventive Intelligence

The central contribution of this article is to distinguish between identifying red flags and using them intelligently.

A red flag is an indicator of potential risk. Intelligence is the result of processing information so that it can support a decision. Therefore, an organisation should not respond to every red flag in the same manner. Instead, the information should move through a structured process.

The first stage is **collection**. Institutions should have mechanisms through which financial, behavioural, audit, compliance and employee concerns can enter a common risk-management process. Collection should not mean unlimited surveillance. Information should be collected for legitimate institutional purposes and within applicable legal and ethical boundaries.

The second stage is **evaluation**. Each indicator should be assessed according to the reliability of its source, the quality of the underlying information and the possibility of an innocent explanation. This prevents the framework from turning every anomaly into an allegation.

The third stage is **corroboration**. An indicator becomes more significant when supported by independent information. For example, a suspicious payment should be examined alongside vendor records, approval trails, related-party information and supporting documentation rather than being treated as suspicious solely because its amount appears unusual.

The fourth stage is **pattern recognition**. The question changes from "Is this transaction unusual?" to "What does this transaction mean when viewed with other events?" A single irregularity may be accidental. Repeated irregularities involving the same vendor, employee, approval mechanism or reporting period may indicate a larger control problem.

The fifth stage is **risk assessment**. Institutions should consider factors such as the reliability of the information, potential financial impact, seniority of the persons involved, vulnerability of the relevant control, repetition of the behaviour and possibility of continuing loss.

The sixth stage is **escalation**. A credible pattern should reach the appropriate authority rather than remaining with the individual who first identified it. This may involve internal audit,

compliance officers, an audit committee, a fraud-risk committee or senior management depending upon the nature and seriousness of the risk.

The seventh stage is **preventive intervention**. Depending on the circumstances, this may involve strengthening controls, increasing transaction review, conducting an independent audit, preserving records, restricting particular processes or commencing a formal investigation.

The final stage is **review and feedback**. The institution should examine whether the response was effective and whether the indicators themselves need to be modified. Intelligence systems should learn from both detected fraud and false alarms.

An Intelligence-Led Fraud Prevention Framework

The proposed framework can therefore be organised into eight stages:

Risk Mapping: Identify areas most vulnerable to fraud, including procurement, lending, financial reporting, related-party transactions and cash management.

Indicator Collection: Collect financial, behavioural, procedural and organisational indicators from legitimate internal and external sources.

Source Evaluation: Evaluate the reliability of the source and the accuracy of the information. Anonymous allegations, automated alerts and documented audit findings should not automatically receive identical weight.

Corroboration and Pattern Recognition: To compare the indicators across transactions, departments, different individuals and time periods. Independent confirmation should be preferred wherever possible.

Threat Assessment: To properly assess the likelihood and potential impact of continuing misconduct while expressly recognising uncertainty.

Escalation: Establish clear thresholds identifying when an issue should move from ordinary monitoring to a compliance review, internal audit, or formal investigations.

Preventive Intervention: To take appropriate action aimed specifically at preventing further loss while preserving the records and avoiding premature conclusions.

Review and Feedback: Evaluate the outcome, identify weaknesses in the system and update the indicators and controls accordingly.

The Indian regulatory framework provides an excellent example of how some of these principles can operate in practice. The RBI's 2024 Master Directions require regulated units to establish Early Warning Signal and Red Flagging frameworks. For banks, a Red Flagged Account is one where one or more early warning indicators raise suspicion and trigger deeper investigation and preventive measures. The framework is subjected to Board-level oversight and validation.

The significance of this approach lies in the fact that an early warning signal does not automatically become a finding of fraud. It initiates further scrutiny. This is consistent with the central argument of this article: the purpose of intelligence is not to declare guilt but to improve the timing and quality of institutional decision making.

Governance, Whistleblowing and Escalation

An intelligence framework cannot function if the institution has no safe route through which information can move.

Section 177 of the Companies Act, 2013 requires listed companies and prescribed classes of companies to establish a vigil mechanism through which directors and employees may report genuine concerns. It also requires safeguards against victimisation and provides for direct access to the Chairperson of the Audit Committee in appropriate or exceptional cases. Similarly, Regulation 22 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 requires listed entities to establish a vigil mechanism or whistleblower policy with safeguards against victimisation.

These mechanisms matter because a warning is useful only if someone is willing and able to communicate it. Fear of retaliation, unclear reporting structures, conflicts of interest and management interference can cause an institution to lose information before it ever reaches the people responsible for acting upon it.

The RBI's 2024 framework similarly places fraud-risk management within governance structures and strengthens the role of Boards, senior management, early warning mechanisms and data analytics. This demonstrates an important shift from viewing fraud as an isolated

compliance incident towards treating it as an institutional risk-management issue.

Intelligence Is Not Evidence

The greatest safeguard required by the proposed framework is a clear distinction between intelligence and evidence.

Intelligence answers questions such as: What appears unusual? What information is reliable? Are multiple indicators connected? What risk requires attention? Evidence, by contrast, must satisfy the requirements applicable to the particular legal, disciplinary or investigative process in which it is used.

This distinction becomes particularly important where the consequences of a fraud classification are serious. In *State Bank of India v. Rajesh Agarwal* (2023), the Supreme Court held that the principles of natural justice had to be read into the process of classifying an account as fraudulent because such classification could have serious civil consequences.

The legal position has since developed further. In *State Bank of India v. Amit Iron Private Limited* (2026), the Supreme Court clarified that *Rajesh Agarwal* did not create an independent right to an oral or personal hearing before fraud classification. At the same time, the Court recognised the importance of procedural fairness and held that relevant audit reports should be furnished where they form the basis of the classification.

This development is valuable to the proposed framework because it illustrates the difference between early detection and final determination. An institution must be able to act upon credible risk without waiting for a court to establish fraud. However, that flexibility cannot justify arbitrary classification, reputational punishment or denial of procedural safeguards.

Preventive intelligence should therefore trigger scrutiny, not substitute for proof.

Risks and Ethical Limits

An intelligence-led framework can itself become harmful if poorly designed.

The first danger is **false positives**. Legitimate business decisions may appear unusual, and employees may display behavioural indicators for reasons unrelated to fraud. An organisation that treats every unusual behaviour as suspicious risks creating an atmosphere of distrust.

The second is **confirmation bias**. Once an individual is flagged, subsequent information may be interpreted selectively as evidence against that person. Institutions must therefore encourage analysts to consider alternative explanations and contradictory information.

The third is **reputational harm**. Confidential intelligence should not be treated as a public accusation. A suspicion recorded for internal risk assessment is fundamentally different from a finding of misconduct.

The fourth is **surveillance overreach**. Data analytics can identify relationships and anomalies at a scale that human reviewers cannot. But technological capability should not become an excuse for unlimited employee monitoring or collection of irrelevant personal information.

The fifth is **automation bias**. A software-generated alert may look objective because it is numerical, but an algorithm can only identify what it has been designed to identify. Data quality, assumptions and thresholds can all produce misleading results.

The sixth is the possibility of **retaliation against whistleblowers**. A system that encourages reporting without protecting those who report simply creates a more sophisticated method of identifying people who can subsequently be silenced.

The framework must therefore be governed by proportionality, confidentiality, need-to-know access, documented reasoning, human review and procedural fairness. Intelligence should remain a decision-support mechanism rather than an automated declaration of guilt.

Conclusion

Financial fraud becomes particularly dangerous when warning signs exist but remain disconnected. The problem is therefore not always a complete absence of information. It may instead be the failure to evaluate, connect and escalate information before the institution reaches a point of crisis.

This article has proposed an intelligence-led approach to that problem. The approach begins with risk mapping and collection of financial, behavioural and organisational indicators. It then requires evaluation of sources, corroboration, pattern recognition and risk assessment before escalation and preventive intervention. Finally, the process must be reviewed so that institutions learn from both genuine fraud and false alarms.

The Indian regulatory framework demonstrates that early warning signals and red-flagging can form part of formal fraud-risk governance, while Indian company and securities regulation recognise the importance of audit committees and protected reporting mechanisms. Recent Supreme Court jurisprudence further demonstrates why early suspicion must remain distinct from final legal determination.

The proposed framework therefore does not claim that institutional collapse can always be prevented. Nor does it suggest that every red flag will lead to fraud. Its more limited and practical claim is that institutions should not wait for certainty before responding to credible risk.

The central movement is consequently not from suspicion to accusation, but from **information to disciplined judgment**:

red flag → evaluation → corroboration → pattern → risk assessment → escalation → prevention.

Preventive intelligence, properly understood, is not panic before proof. It is disciplined institutional judgment before the cost of discovering the truth becomes irreversible.

REFERENCES:

1. Association of Certified Fraud Examiners. (2020). *Behavioral red flags of fraud*. ACFE.

2. Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. ACFE.

3. Committee of Sponsoring Organizations of the Treadway Commission, & Association of Certified Fraud Examiners. (2023). *Fraud risk management guide* (2nd ed.).

4. Heuer, R. J. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence, Central Intelligence Agency.

5. National Financial Reporting Authority. (2023). *Statutory auditors' responsibilities in relation to fraud in a company*. NFRA.

6. Public Company Accounting Oversight Board. (2024). *AS 2401: Consideration of fraud in a financial statement audit*. PCAOB.

7. Reserve Bank of India. (2024). *Master directions on fraud risk management in commercial banks (including regional rural banks) and all India financial institutions*. RBI.

8. Reserve Bank of India. (2024). *Master directions on fraud risk management for non-banking financial companies*. RBI.

9. Reserve Bank of India. (2024). *RBI issues revised Master Directions on Fraud Risk Management in the Regulated Entities*. RBI.

10. Reserve Bank of India. (2025). *FAQs on Master Directions on Fraud Risk Management in Regulated Entities, 2024*. RBI.

11. Securities and Exchange Board of India. (2015, as amended). *SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015*. SEBI.

12. Securities and Exchange Board of India. (2015). *SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015*, Regulation 22. SEBI.

13. United Nations Office on Drugs and Crime. (2011). *Criminal intelligence: Manual for analysts*. United Nations.

14. United Nations Office on Drugs and Crime. (2011). *Criminal intelligence for managers*. United Nations.

15. Federal Bureau of Investigation. (n.d.). *White-collar crime*. FBI.

16. Cornell Law School Legal Information Institute. (n.d.). *White-collar crime*. Legal Information Institute.

17. *State Bank of India v. Rajesh Agarwal*, (2023) 6 SCC 1.

18. *State Bank of India v. Amit Iron Private Limited*, 2026 INSC 323.

19. Companies Act, 2013, 177.

20. Securities and Exchange Board of India. (2015, as amended). *SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015*, Regulation 22.