cyril amarchand mangaldas
ahead of the curve

Fraud Investigation in India

A Cyril Amarchand Mangaldas Thought Leadership Publication

Disclaimer:

The handbook has been prepared for informational purposes only and nothing contained in this handbook constitutes legal or any other form of advice from Cyril Amarchand Mangaldas. Although reasonable care has been taken to ensure that the information in this Hand Book is true and accurate, such information is provided 'as is', without any warranty, express or implied as to the accuracy or completeness of any such information.

Cyril Amarchand Mangaldas shall not be liable for any losses incurred by any person from any use of this publication or its contents. The position of law expressed here are only valid as on May 30, 2022.

A Thought Leadership Publication

We now present this handbook to enable readers to have an overview of the systems and legal rules and regulations that are essential for business operations in India.

"More money has been stolen at the point of a pen - than at the point of a gun."

- Frank Schmalleger (1991)

Professor Emeritus at the University of North Carolina at Pembroke.

Content

1	Understanding Fraud	05
2	The Law on Fraud	07
3	Investigating Fraud	11
4	Meaning and Significance of Forensic Audit	15
5	Beginning to Identity and Detect Fraud, its Symptoms	21
6	Organisational Indicators	22
7	Red Flags	23
8	Whistle Blower Complaints and How to Deal with Them	25
9	Investigating Purported Fraud	32
10	Understanding Fraud Measures in the Organizations	35
11	Considering Gaps In Internal Control Structure	38
12	Crisis Management	41
13	Legal Privilege and Investigations	44
	ANNEXURE - A	50
	ANNEXURE - B	51

A

Understanding Fraud

Brief History of Fraud

The first instance of financial fraud was recorded in ancient Greece in 300 BC. Hegestratos, a shipping merchant, attempted to defraud the insurers of a shipload of valuable goods by sinking his boat but keeping the cargo and claiming the loss anyway.

In the early days of common law, fraud and misrepresentation were easily seen as cheating or false projection on the part of one of the contracting parties. For a long time, there was no liability in tort for an intentionally rendered false declaration, and it was believed that a reckless person is not a dishonest one. However, the ambit and importance of fraud became more precise after the case of *Derry v. Peek.*[1], a landmark case which led to the evolution of concepts of fraud and misrepresentation under common law. In the said case, Lord Herschell determined that a statement would be fraudulent when it was made – knowingly, or without belief in its truth, or recklessly / carelessly whether it be true or false.

Fraud under Indian Law

Meaning of 'Fraud'

The Black's Law Dictionary defines 'fraud' as 'a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.'[2] In the explanation to section 447 of the Companies Act, 2013 (the "**Act**"), the term 'fraud' is defined as "*any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss.*" Sec. 447 is an amalgam of several sections of the Indian Penal Code, 1860 ("**IPC**") including Sec. 405 (criminal breach of trust), Sec. 415 (cheating), Sec. 463 (forgery) and Sec. 477A (falsification of accounts). The IPC does not explicitly define 'fraud', however, under Section 25 of the IPC, the statute defines 'fraudulently' to mean "*a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.*"

[1] (1889) 14 App Cas 337.

[2] Black's Law Dictionary, 9th ed., Bryan A. Garner, West Publishing Co., St. Paul, Minnesota, 2009.

SA 240 issued by ICAI, deals with the auditor's responsibilities towards frauds in the financial statement audits and explains processes and methodology for identification, assessment and procedures for detection of fraud in the financials. SA 240 defines 'fraud' as "a*n intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage*."[3]

Other definition of fraud in the Indian legal context has been provided under **Annexure A** to this note.

[3] Naman Desai, Understanding the Theoretical Underpinnings of Corporate Fraud, JDM, 45(1) 25–31, 2020.

B

The Law on Fraud

Fraud under Companies Act 2013

Fraud is a penal offence and is punishable with fine and imprisonment (or fine/ imprisonment) under Section 447 of the Act. The various penal thresholds are as below:

Punishment for fraud

447. Without prejudice to any liability including repayment of any debt under this act or any other law for the time being in force, any person who is found to be guilty of fraud involving an amount of at least ten lakh rupees or one per cent of the turnover of the company, whichever is lower shall be punishable with **imprisonment for a term which shall not be less than six months** but which may extend to ten years **and shall also be liable to fine** which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud.

Provided that **where the fraud in question involves public interest, the term of imprisonment shall not be less than three years.**

Provided further that where the fraud involves an amount less than ten lakh rupees or one per cent of the turnover of the company, whichever is lower, and does not involve public interest, any person guilty of such fraud shall be punishable with **imprisonment for a term which may extend to five years or with fine which may extend to fifty lakh rupees or with both.**

Explanation. — for the purposes of this section —

i. "fraud" **in relation to affairs of a company or anybody corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any** wrongful gain or wrongful loss;

ii. "wrongful gain" means the gain by unlawful means of property to which the person gaining is not legally entitled;

iii. "wrongful loss" means the loss by unlawful means of property to which the person losing is legally entitled.

The relevant sections under the Act that attract liability u/s 447 have been tabulated under **Annexure B** to this note.

Standard of proof for Fraud

As fraud committed under Section 447 of the Act is a criminal offence, the standard of proof to establish fraud is similar to the standard of proof applicable to other criminal offences; in such cases, the standard of proof is 'beyond reasonable doubt'. The Supreme Court and the Bombay High Court have held that fraud like any other charge of a criminal proceeding must be established beyond reasonable doubt. Further, a finding as to fraud cannot be based on suspicion and conjecture and the material and evidence have to prove the fraud.

The Supreme Court in *Union Of India vs. Chaturbhai M. Patel and Co.*[4] has held that: "**It is well settled that fraud like any other charge of a criminal offence whether made in civil or criminal proceedings, must be established beyond reasonable doubt**: per Lord Atkin in ***A.L.N. Narayanan Chettyar v. Official Assignee, High Court, Rangoon***[5] however suspicious may be the circumstances, however strange the coincidences, and however grave the doubts, suspicion alone can never take the place of proof. In our normal life we are sometimes faced with unexplainable phenomenon and strange coincidences, for as it is said, truth is stronger than fiction. In these circumstances, therefore, after going through the judgment of the high court we are satisfied that the appellant has not been able to make out a case of fraud as found by the high court. As such the high court was fully justified in negating the plea of fraud and in decreeing the suit of the plaintiff."

The Supreme Court in the case of *Svenska Handelsbanken vs. Indian Charge Chrome and Ors.*[6] cited the following excerpt: "In A.L.N. Narayanan Chettiyar and Anr. v. Official Assignee, High Court Rangoon and Anr., the Privy Council held that "**fraud like any charge of a criminal proceedings, must be established beyond reasonable doubt**. A finding as to fraud cannot be based on suspicion and conjecture"

The Bombay High Court in the case of *Kisan Sahakari Chini Mills Limited vs. Richardson And Cruddas* held that: "the nature of fraud is fraud of an egregious nature as to vitiate the entire underlying transaction. It is fraud of the beneficiary, not the fraud of somebody else. There must be a specific plea of fraud. The party alleging fraud must necessarily plead and produce all necessary evidence in proof of the fraud in execution of the contract of guarantee. **Moreover, fraud like any other charge of a criminal proceeding must be established beyond reasonable doubt. A finding as to fraud cannot be based on suspicion and conjecture. The material and evidence have to show it**."[7]

The Bombay High Court in *Sant Chemicals Pvt. Ltd. vs. Sant Chemicals Pvt. Ltd. And Ors.* also mentioned that **it is a settled proposition of law that fraud must be proved beyond reasonable doubt**; the court could not simply proceed merely on suspicions, conjectures and surmises. There must be clear and cogent evidence to show beyond reasonable doubt that fraud has indeed been committed on the court.[8]

---

[4] Union of India vs. Chaturbhai M. Patel and Co. (AIR 1976 SC 712)
[5] A.L.N. Narayanan Chettyar v. Official Assignee, High Court, Rangoon (AIR 1941 PC 93)
[6] Svenska Handelsbanken vs. Indian Charge Chrome and Ors. (AIR 1994 SC 626)
[7] Kisan Sahakari Chini Mills Limited vs. Richardson And Cruddas (AIR 1997 BOM 35)
[8] Sant Chemicals Pvt. Ltd. vs. Sant Chemicals Pvt. Ltd. And Ors. (999 (3) All MR 680)

The Bombay High Court in the case of *Akai Impex Ltd. vs. General Steel Export and Ors.* held that: "the nature of fraud is fraud of an egregious nature as to vitiate the entire underlying transaction. It is fraud of the beneficiary, not the fraud of somebody else. There must be a specific plea of fraud. The party alleging fraud must necessarily plead and produce all necessary evidence in proof of the fraud. Fraud like any other charge of a criminal proceeding must be established beyond reasonable doubt. A finding as to fraud cannot be based on suspicion and conjecture".[9]

In the context of establishing the commission of an offence, the word 'fraud' constitutes – (a) deceit or an intention to deceive; and (b) injury to someone because of such deceit.[10] While deciding a case pertaining to the offence of forgery under IPC, the Supreme Court of India in ***Vimla vs Delhi Administration***[11] held- *"... the idea of deceit is a necessary ingredient of fraud, but it does not exhaust it; an additional element is implicit in the expression..." this additional element i.e. 'injury' "is something other than economic loss that is deprivation of property, whether movable or immovable or of money and it will include any harm whatever caused to any person in body, mind, reputation or such others."*

A benefit or advantage to the deceiver will almost cause a loss or detriment to the deceived. Even in those rare cases where there is a benefit or advantage to the deceiver, but no corresponding loss to the deceived, the second requirement (injury) is satisfied.

A full bench of Madras High Court in *Kotamraju Venkatrayadu v. Emperor*[12] illustrated the elements of fraud in the following manner –

"*a tells b a lie and b believes him. B is deceived but it does not follow that a intended to defraud b. But, as it seems to me,* ***if a tells b a lie intending that b should do something which a conceives to be to his own benefit or advantage, and which, if done, would be to the loss or detriment of b, a intends to defraud b."***

Meaning of the term 'Beyond Reasonable Doubt'

Supreme Court in *State of Madhya Pradesh Vs. Dharkole Alias Govind*[13] in its judgment has observed as under:-

> *"A person has, no doubt, a profound right not to be convicted of an offence which is not established by the evidential standard of proof beyond reasonable doubt. Though this standard is a higher standard, there is, however, no absolute standard.* ***What degree of probability amounts to 'proof' is an exercise particular to each case? Referring to probability amounts to 'proof' is an exercise the inter-dependence of evidence***

[9] Akai Impex Ltd. vs. General Steel Export and Ors.

[10] Vimla vs Delhi Administration, AIR 1963 SC 1572; Dr. S. Dutt v. State of Uttar Pradesh, AIR 1966 SC 523.

[11] Ibid.

[12] Kotamraju Venkatrayadu v. Emperor (1905) I.L.R. 28 Mad. 99, 96, 97.

[13] State of Madhya Pradesh Vs. Dharkole Alias Govind AIR 2005 SC 44

and the confirmation of one piece of evidence *by another a learned author says: (see "the mathematics of proof ii": Glanville Williams: Criminal Law Review, 1979, By Sweet And Maxwell, P.340 (342).*

"10. the simple multiplication rule does not apply if the separate pieces of evidence are dependent. Two events are dependent when they tend to occur together, and the evidence of such events may also be said to be dependent. In a criminal case, different pieces of evidence directed to establishing that the defendant did the prohibited act with the specified state of mind are generally dependent. A junior may feel doubt whether to credit an alleged confession, and doubt whether to infer guilt from the fact that the defendant fled from justice. But since it is generally guilty rather than innocent people who make confessions and guilty rather than innocent people who run away, the two doubts are not to be multiplied together. The one piece of evidence may confirm the other.

11. Doubts would be called reasonable if they are free from a zest for abstract speculation. Law cannot afford any favourite other than truth. To constitute reasonable doubt, it must be free from an over emotional response. Doubts must be actual and substantial doubts as to the guilt of the accused persons arising from the evidence, or from the lack of it, as opposed to mere vague apprehensions. ***A reasonable doubt is not an imaginary, trivial or a merely possible doubt; but a fair doubt based upon reason and common sense. It must grow out of the evidence in the case.***

12. The concepts of probability, and the degrees of it, ***cannot obviously be expressed in terms of units to be mathematically enumerated as to how many of such units constitute proof beyond reasonable doubt.*** *There is an unmistakable subjective element in the evaluation of the degrees of probability and the quantum of proof.* ***Forensic probability must, in the last analysis, rest on a robust common sense and, ultimately, on the trained intuitions of the judge.*** *While the protection given by the criminal process to the accused persons is not to be eroded, at the same time, uninformed legitimization of trivialities would make a mockery of administration of criminal justice."*

Supreme Court in *Gurbachan Singh v. Satpal Singh And Others*[14] in its judgment has observed as under: - "*the conscience of the court can never be bound by any rule but that is coming itself dictates the consciousness and prudent exercise of the judgment*. **Reasonable doubt is simply that degree of doubt which would permit a reasonable and just man to come to a conclusion.** *Reasonableness of the doubt must be commensurate with the nature of the offence to be investigated.*"

[14] Gurbachan Singh v. Satpal Singh And Others AIR 1990 SC 209.[7] Sant Chemicals Pvt. Ltd. vs. Sant Chemicals Pvt. Ltd.

C

Investigating Frauds

Serious fraud investigation office ("SFIO")

SFIO was created to grant Ministry of Corporate Affairs (**MCA**) powers to investigate serious frauds and offences relating to a company under Sec. 447 of the Act, without depending on police investigation under the IPC. SFIO consists of experts in the field of accountancy, forensic auditing, law, information technology, investigation, company law, capital market and taxation for detecting / prosecuting / recommending for prosecution white-collar crimes / frauds.

Sec. 211 of the Act provides for establishment of SFIO by Central Government ("**CG**"). As per Section 212(1) of the Act, CG has discretion to order an investigation into the affairs of a company – (a) on the receipt of a report of the registrar / inspector; (b) on intimation of a special resolution passed by a company; (c) in public interest; or (d) on request of any department of CG or State Government.

Role / Importance of SFIO

SFIO takes up fraud investigation under the Act in those cases, which are characterized by –

i. Complexity and having inter-departmental / multi- disciplinary ramifications.

ii. Substantial involvement of public interest – in terms of monetary misappropriation or no. of persons affected, and

iii. The possibility of investigation leading to a clear improvement in systems, laws, or procedures.[15]

Similar to its counterpart in the United Kingdom (where the serious fraud office collaborates with other agencies such as the financial conduct authority and the economic crime directorate), the SFIO in India works closely with the other law enforcement agencies such as the Economic Offences Wing of the State Police, the Central Bureau of Investigation (**CBI**), the Directorate of Enforcement (**ED**), Income Tax Department etc. for early detection and speedy investigation of corporate frauds.

[15] About SFIO History, available at: https://sfio.nic.in/about_history_sfio.

Powers of SFIO

SFIO enjoys exclusive jurisdiction[16] and powers of inspector (including power to arrest[17]) under sec. 217 of the Act and enjoys all the powers as are vested in a civil court under the Code of Civil Procedure, while trying a suit in respect of:-

i. Discovery and production of books of account and other documents, at such place and time as may be specified by such person; substantial involvement of public interest – in terms of monetary misappropriation or no. of persons affected, and

ii. Summoning and enforcing the attendance of persons and examining them on oath (and using the statement against the person as an evidence)[18]; and

iii. Inspection of any books, registers, and other documents of the company at any place.

On completion of the investigation, SFIO submits the final investigation report to CG. CG, after examination, may direct the SFIO to initiate prosecution against the company / its officers or employees.

Statistics of cases investigated[19]

Financial year	Probes conducted	Companies involved
FY 2019-2020	12 probes	361 companies
FY 2018-2019	12 probes	83 companies
FY 2017-2018	5 probes	132 companies

[16] Section 212(2).
[17] MCA Notification dt. 24th August, 2017, available at: https://www.mca.gov.in/Ministry/pdf/companiesArrestsconnectionSFIORule_25082017.pdf
[18] Section 217(7).
[19] SFIO completed investigations against 361 companies last fiscal: Government, available at: https://economictimes.indiatimes.com/news/politics-and-nation/sfio-completed-investigations-against-361-companies-last-fiscal-government/articleshow/78126455.cms?from=mdr.

Key investigations:

a. Satyam scam

SFIO's report in Satyam scam ran into 12,000 pages, in 30 volumes and was submitted before the mandate of 3-months.[20] SFIO had investigated / interrogated the directors and opined that the fraud was done allegedly by the chairman and top executives of the company. The SFIO opined that the accountants, instead of using independent testing mechanism, used the tools of Satyam and were negligent in performing their statutory duties and reporting standards. The investigation eventually led to the founder of Satyam computers (Mr. Ramalinga Raju) and his brothers being sentenced to 7 years in jail and being fined Rs. 5.5 crore.

b. Saradha chit fund scam

Saradha group ran a chit fund in West Bengal and had collected around Rs. 200 to 300 billion from investors. SFIO investigation concluded that the group was using collections from new investors to make payments to the past enrolled members, rather than from income through investments, in typical resemblance to a *Ponzi* scheme.[21] Currently, the case is pending with the CBI which received the case in May 2014 after the Supreme Court ordered investigation pursuant to a PIL.[22]

c. Some ongoing SFIO investigations

SFIO is currently investigating in the 114 companies which are directly or indirectly linked to Nirav Modi and Mehul Choksi regarding the PNB scam.[23] SFIO is also investigating TRS MP Nama Nageswara Rao for misusing bank loans taken for the Madhukan company's national highway project in Jharkhand.[24] The investigation of Fortis for the recovery of Rs. 500 crores from Singh brothers (who are accused of diverting Religare's money and investing in other companies) is also currently being handled by the SFIO.[25]

---

[20] SFIO concludes Satyam probe, available at: https://www.business-standard.com/article/companies/sfio-concludes-satyam-probe-109041500042_1.html.s.

[21] Saradha group cos will face prosecution for violation of several laws: SFIO, available at: https://www.thehindubusinessline.com/news/saradha-group-cos-will-face-prosecution-for-violation-of-several-laws-sfio/article20864838.ece1.

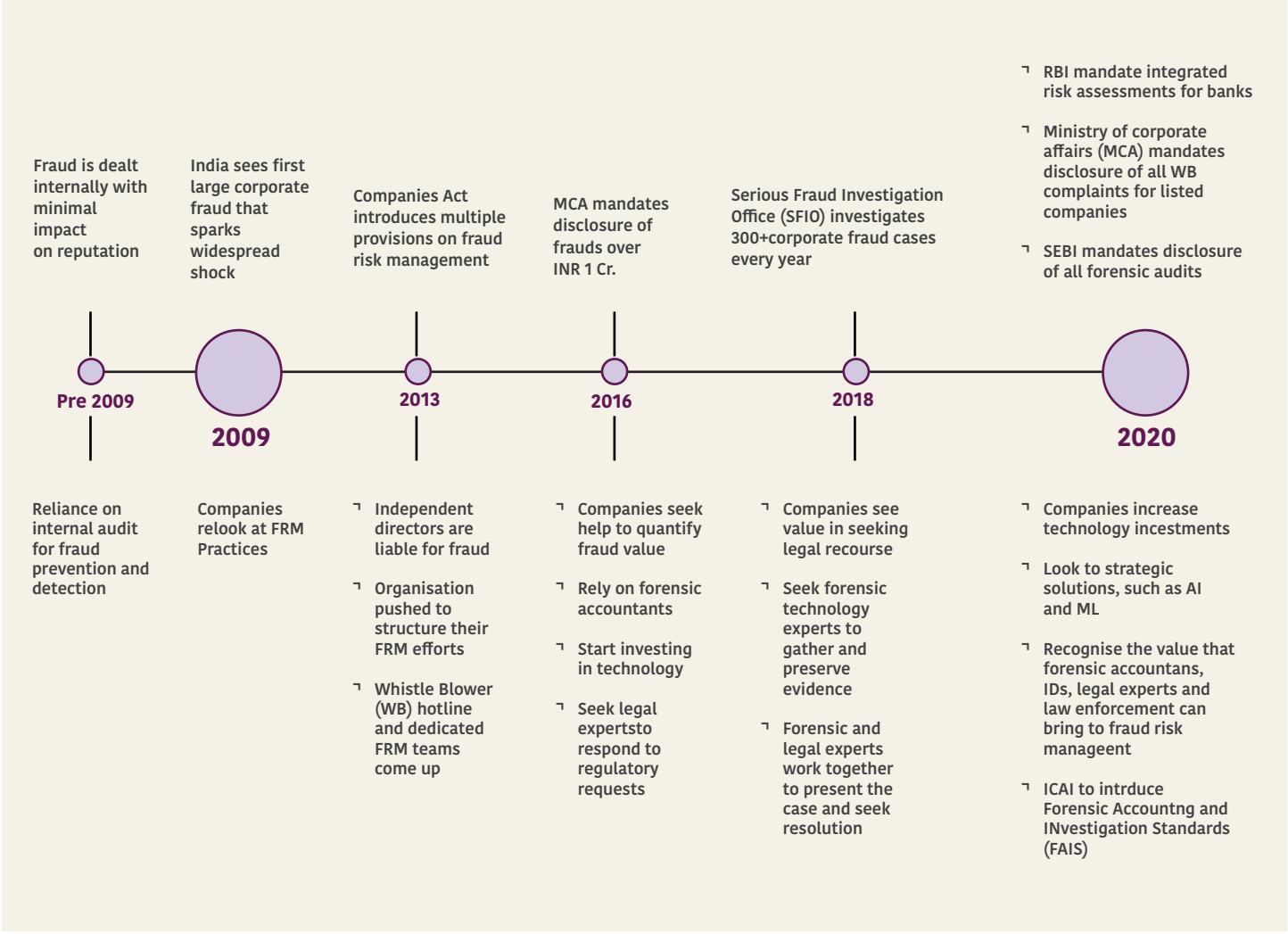
[22] Seven years on, CBI still silent on Saradha chit fund scam, available at: https://www.sundayguardianlive.com/news/seven-years-cbi-still-silent-saradha-chit-fund-scam.

[23] https://www.sundayguardianlive.com/news/seven-years-cbi-still-silent-saradha-chit-fund-scam

[24] Nama Nageswara Rao clarifies that he will cooperate for ED investigation, available at: https://www.thehansindia.com/telangana/nama-nageswara-rao-clarifies-that-he-will-cooperate-for-ed-investigation-691553.

[25] HC allows SFIO to interrogate Singh brothers for two weeks starting Jan 1, available at: https://economictimes.indiatimes.com/industry/banking/finance/hc-allows-sfio-to-interrogate-singh-brothers-for-two-weeks-starting-jan-1/articleshow/79958437.cms?from=mdr.

The evolution of anti-fraud ecosystem in India can be represented by way of the following diagram[26]:



[26] Deloitte, India Corporate Fraud Perception Survey Edition IV (December 2020), available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-india-corporate-fraud-perception-survey-edition-IV.pdf.

D

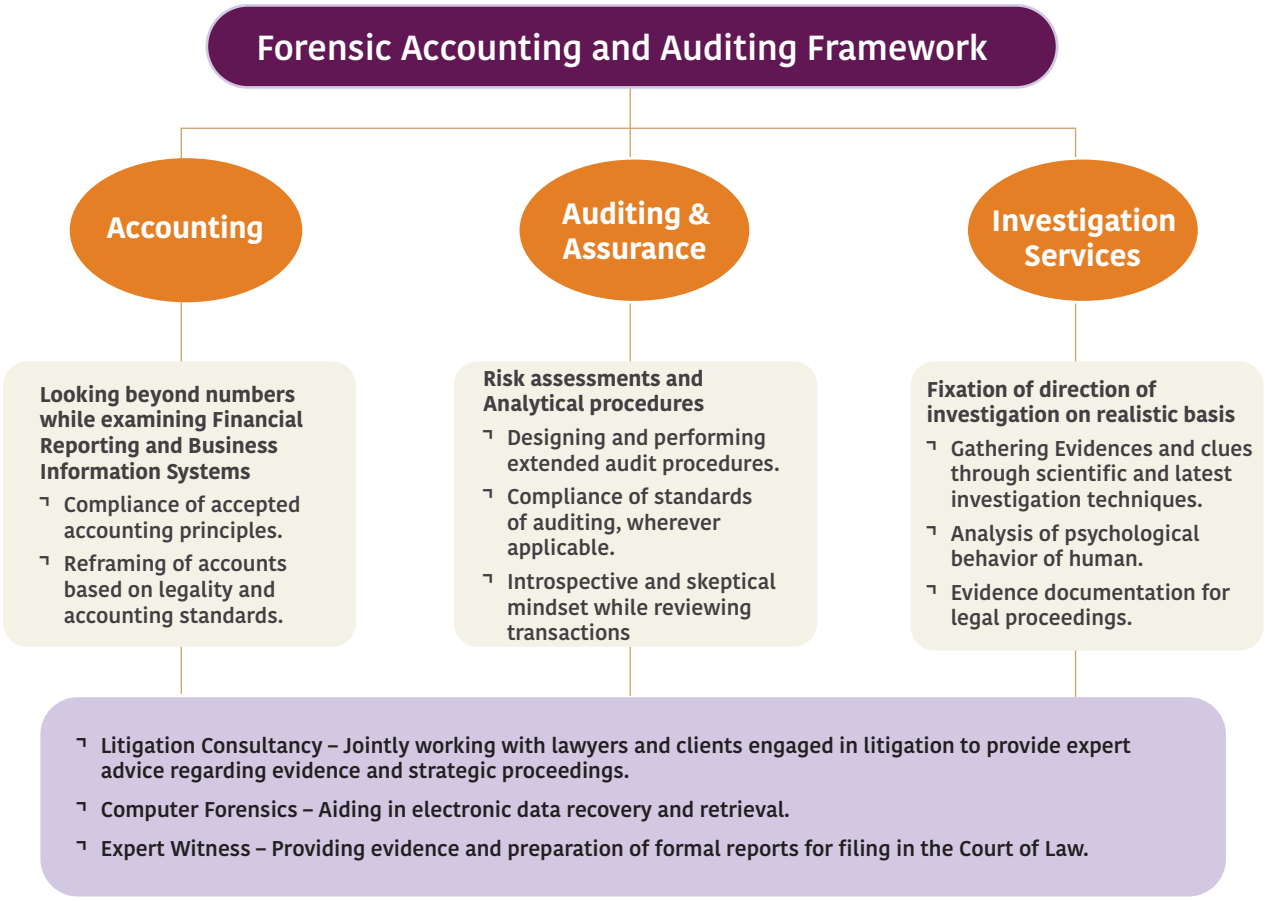
Meaning and Significance of Forensic Audit

Background

Forensic audit involves examination of past financial records of an entity to detect any illegal action, manipulation in the books of accounts, siphoning of funds, etc. **Unlike financial audits which are focused more on statutory compliance, the forensic audits are designed to investigate the financial records of an entity to derive evidences in support of fraud that can be used in court of law or legal proceedings.**

Collin Greenland notes that forensic accounting (or auditing) is the **integration of accounting, auditing and investigative skills** in order to provide an accounting analysis suitable for the resolution of disputes (usually, but not exclusively) in the courts.[27] With the increase in financial fraud popularly known as white-collar crime, forensic auditing and accounting has emerged as an apt tool to ensure financial health of the companies through **aiding in the prevention, regulation and penalization of financial frauds and scams.**

The forensic accounting and auditing framework can be illustrated as below:



[27] Deloitte, India Corporate Fraud Perception Survey Edition IV (December 2020).

Effect of forensic accounting/auditing in prevention of fraud

A study conducted to examine the importance of forensic accounting suggests that **there is significant positive effect of forensic accounting in the detection and prevention of financial frauds in India.**[28] The respondents surveyed in the above study gave positive response with respect to the following statements –

a. Forensic accounting can be used to locate diverted funds or assets.

b. Forensic accounting can identify misappropriated funds or assets.

c. Financial statements frauds are reduced to minimal level with the help of forensic accounting.

Forensic accounting / auditing played a major role in scams like Stamp paper scam, Satyam scam, 2G spectrum, Commonwealth games etc.[29]

Regulatory stance on forensic auditing

Various regulatory stipulations in relation to forensic auditing can summarised as below:

Companies Act, 2013	Fraud investigation u/s 212 of the Act by SFIOs involve forensic audits by the concerned regulators to unveil potential fraud.
SEBI (LODR) Regulations, 2015	In case of initiation of forensic audit, the following disclosures shall be made to the stock exchanges (without any application of materiality threshold) by the listed entities: a. The fact of initiation of forensic audit along-with name of entity initiating the audit and reasons for the same, if available; and b. Final forensic audit report (other than for forensic audit initiated by regulatory / enforcement agencies) on receipt by the listed entity along with comments of the management, if any.
RBI's Master Direction on frauds – classification and reporting by commercial banks and select FIs[30]	RBI has made forensic audit mandatory for large advances and restructuring of accounts.

[28] Ridhi Gupta, 'Financial Frauds and Forensic Accounting: Empirical Evidences from Indian Corporate Sector', available at: https://www.ijcrt.org/download.php?file=IJCRT2102196.pdf.

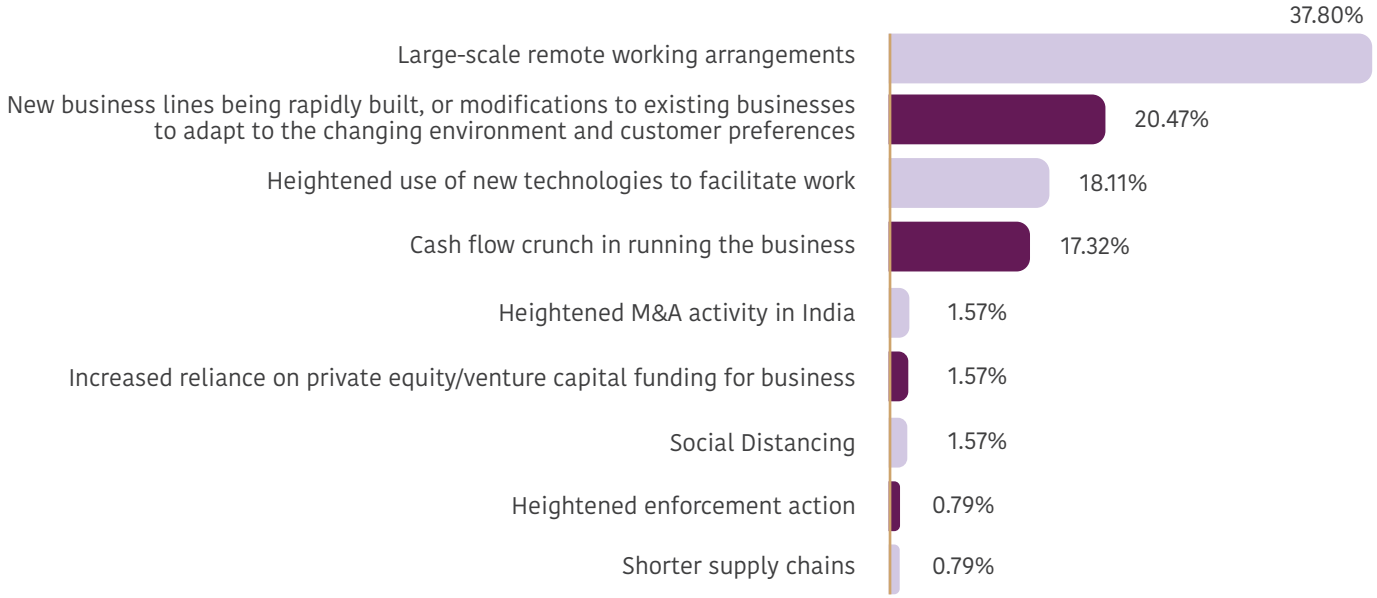
[29] Sana Moid, 'Application of Forensic Accounting to Investigate Scams in India, available at: https://mba.mits.ac.in/MIJBR/Article%204%20Sana%20-%20Forensic%20Accounting.pdf.

[30] Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, Master Circular No. RBI/DBS/2016-17/28 DBS.CO.CFMC.BC.No.1/23.04.001/2016-17 dated 1st July 2016.

Prevention of Money Laundering Act (PMLA)	Activities like placement of fund (including cash), structuring and layering, integration and finally carrying such fund to tax heaven foreign countries etc. evince the scope of integration of forensic audit processes with investigations conducted under the PMLA.
Insolvency and Bankruptcy Code, 2016	Insolvency professionals (IPs) are obligated to avoid fraudulent or wrongful transactions. The unearthing and reporting of transactions of questionable nature is usually done by IPs through forensic methodologies such as data analytics, document review, market intelligence, etc.[31]
Market regulators	SEBI for securities market and IRDAI for insurance sector, investigate the affairs of intermediaries / insurers to regulate and supervise their respective markets by appointing independent auditors to conduct forensic audits of companies.
Indian Evidence Act, 1872	Section 45 and 47 support the report of forensic auditors.

Recent trends

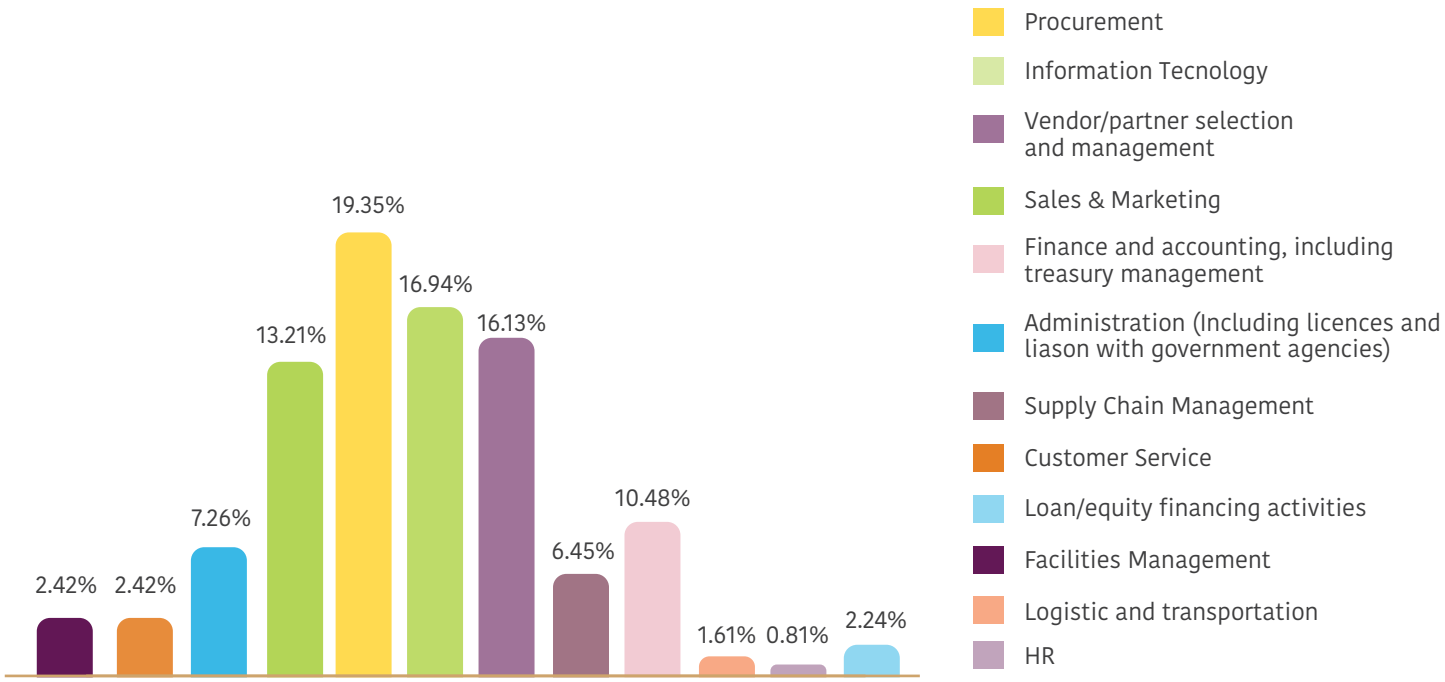
The recent December 2020 fraud perception survey by Deloitte ("**Deloitte 2020 survey**")[32] indicates that the top three future trends with a potential to significantly impact corporate frauds are: (a) large-scale remote working arrangements (37.80 percent); (b) rapid changes in the current business and launch of new businesses (20.47 percent), and (c) heightened use of new technologies to facilitate work (18.11 percent).



[31] Section 43 to 51 and 66 of IBC, 2016.

[32] Deloitte, India Corporate Fraud Perception Survey Edition IV (December 2020), available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-india-corporate-fraud-perception-survey-edition-IV.pdf.

The Deloitte 2020 survey also suggests that procurement (19.35 percent) and information technology (16.94 percent) remain processes which are most vulnerable to fraud risks.



Barring famous Indian corporate frauds like Sahara group scam, Satyam computers and ILFS fraud, some recent instances of corporate / bank frauds have forced the regulators / government to conduct forensic audit of the accounts of companies involved by independent auditors. In 2017, the Finance Ministry ordered a forensic audit of Dena bank and Oriental bank of commerce for misappropriation of funds worth Rs. 437 crores, mobilised through fixed deposits.[33] Similarly, in 2021, SEBI conducted a forensic audit of accounts of Suzlon Energy Ltd. and SunEdison Infrastructure to check for violations related to the Act and the securities market.[34]

[33] Beena Parmar, 'Finance Ministry orders forensic audit on Dena Bank', OBC in Rs 437-cr fraud, BusinessLine, November 25, 2017, available at: https://www.thehindubusinessline.com/money-and-banking/Finance-Ministry-orders-forensic-audit-on-Dena-Bank-OBC-in-Rs-437-cr-fraud/article20848451.ece

[34] Mint, Regulator probes Suzlon's accounts, available at: https://www.livemint.com/companies/news/sebi-orders-forensic-audit-of-suzlon-11616497124637.html; The Economic Times, Sebi orders forensic audit of books of SunEdison Infrastructure, available at: https://economictimes.indiatimes.com/markets/stocks/news/sebi-orders-forensic-audit-of-books-of-sunedison-infrastructure/articleshow/80930710.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

Increasing importance of forensic investigations and experts

In investigating corporate frauds, a forensic accountant /auditor performs the following functions[35]:

a. Determines the correctness of the accounting transactions of the institution.

b. Determines the presence / absence of material values and funds.

c. Establishes the validity of posting or writing off material assets and monetary funds.

d. Determines the circumstances related to shortages and surpluses.

e. Determines the soundness of the audit performed.

f. Determines the quantum of material damage caused due to fraudulent activities.

g. Determines the state of accounting in the institution.

h. Determines whether fraud is carried out or the presence/absence of tax evasion.

i. Checks how the assets are divided between the partners.

j. Falsification of documents, etc.

Private forensic investigations remove (or reduce) the possibility of bias and carry out a forensic analysis of the records of the company. Such professionals investigate similar to what may be carried out by investigating authorities if an official complaint were to be registered, allowing the company to be ready for official investigations.

Various investigation agencies such as police, CBI etc. are taking the help of Chartered Accountants/ CWAs as a forensic accountant and using their report as evidence in the cases of criminal/civil nature.

Forensic accountants / auditors as 'experts'

Forensic reports may be admissible as expert evidence before a court of law. Sections 45 to 51 of the Indian Evidence Act, 1872 lay down the provisions relating to expert evidence and third-party witnesses. **Section 45 allows the judge to appoint an expert having specialised**

[35] Forensic Accounting And Fraud Detection: How To Save Your Business At The Right Time?, available at: https://www.cac.net.in/blog/forensic-accounting-and-fraud-detection-how-to-save-your-business-at-the-right-time/.

knowledge, experience or skill in foreign law, **science, art**, handwriting or finger impression **to assist the court in reaching a judgment based on the facts presented before it**. The words 'science' and 'art' have been construed broadly under section 45 to expand its applicability to include the opinion of accountants, etc under its ambit.[36]

Further, Section 2(38) of the Act defines 'expert' to include a chartered accountant, a company secretary and a cost accountant. While the **opinion of an expert** is not binding and its probative value would depend on the corroborative evidence available, the same **is increasingly becoming a reliable tool to prosecute or defend an allegation of white-collar crimes**, especially when justified along with efficient investigative practices.

[36] Basudeo Gir v State, AIR 1959 Pat 534.

E

Beginning to Identity and Detect Fraud, its Symptoms

Parameters	Low Concentration of Fraud	High Concentration of Fraud
Business Focus	Customer Satisfaction	Profit Sensitive
Financial Reporting	Transparent	Complex and Opaque
Leadership Style	Participative	Authoritative
Budgeting	Realistic and Flexible	Aggressive and Stringent
Employee Salary	Market Equivalent	Below market equivalent
Tone at the Top	Strong ethics; Lead by example	Sub-standard governance and ethics
Independence of internal auditors	Reporting to Audit Committee	Reporting to Senior Management leads
Customer Complaints	Few / Nil	Many and repetitive

Paying close attention to some of the most common indicators of fraud can increase the likelihood of the discovery of the fraudster at an early stage. An illustration of the parameters which largely determine the concentration / likelihood of happening of fraud in any business organization can be understood in the following manner:

We can categorize fraud indicators into the following two heads[37]:

a. Organisational indicators
b. Red flags / fraud alerts

[37] Chartered Institute of Management Accountants, 'Fraud risk management: a guide to good practice', pg. 39, available at: https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf

F

Organisational Indicators

Organizational indicators can be further subdivided into sub-categories such as:

- **business risk** [identified through cultural issues like absence of an anti-fraud culture and failure of management to implement a sound system of internal control, or management issues like strained relationships within the organisation, lack of management co-operation with auditors etc., or employee issues like inadequate recruitment processes and absence of screening etc., or process issues like poor management accountability / reporting systems etc., or transaction issues like poor documentary support for specific transactions and large cash transactions etc.];
- **financial risk** [involving issues like complex transactions, use of complex financial products, rapid changes in profitability etc.];
- **environmental risk** [including issues like introduction of new accounting or other regulatory requirements which could significantly alter reported results, rapid technological changes etc]; and
- **it and data risk** [involving breaches in data security and privacy, sensitive data being stolen leaked or lost etc.].

Business Risk	⌝ Cultural issues (like absence of an anti-fraud culture). ⌝ Management issues (like lack of management co-operation with auditors). ⌝ Employee issues (like inadequate recruitment / screening processes). ⌝ Transaction issues (like large cash transactions) etc.
Financial Risk	⌝ Complex transactions. ⌝ Use of complex financial products. ⌝ Rapid changes in profitability. ⌝ Extensive use of tax havens without clear business justification etc.
Environmental Risk	⌝ Introduction of new accounting or other regulatory requirements which could significantly alter reported results. ⌝ Rapid technological changes etc.
IT and Data Risk	⌝ Data security and privacy. ⌝ Sensitive data being stolen leaked or lost etc. ⌝ Unauthorised electronic transfer of funds or other assets. ⌝ Users not adopting good computer security practices, etc.

G

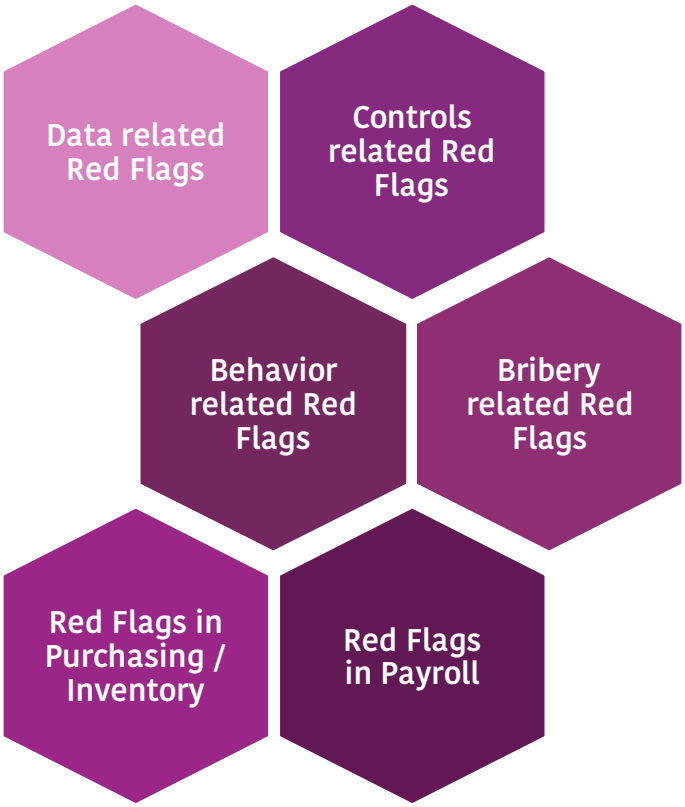
Red Flags

A global survey of 1,483 occupational fraud cases in 2014 reported that ninety-two per cent of fraud cases exhibit some warning signs which are characterised by specific events indicative of fraud.[38] These symptoms signals are known as red flags. A red flag is a set of incidents or circumstances that are uncommon in nature or differ from the normal activity.

Employee Red Flags	¬ Employee lifestyle changes (expensive cars, jewellery, homes, clothes etc.) ¬ Behavioural changes (unusual, irrational, or inconsistent). ¬ Significant personal debt of employees, etc.
Management Red Flags	¬ Reluctance of management to provide information to auditors. ¬ Frequent disputes with auditors. ¬ Managers displaying significant disrespect for regulatory bodies, etc.
Transactional Red Flags	¬ Transactions making no sense considering the company's operations / goals. ¬ An apparent override of internal controls to record the transaction, etc.
Documents related Red Flags	¬ Photocopied or missing documents ¬ Evidence of backdating of documents, etc.

Studies done on fraud cases exhibit that red flags were present in the attending circumstances but were either not recognized or were recognized but not acted upon by the stakeholders involved.

[38] Report to the Nations on Occupational Fraud and Abuse, available at: https://www.acfe.com/rttn/docs/2014-report-to-nations.pdf.



The most common red flags include:

- **employee red flags** (involving employee lifestyle changes such as purchase of expensive cars, jewellery, homes, clothes etc., or behavioural changes in employees, or significant personal debt of employees etc.);
- **management red flags** (for instance, reluctance of the management to provide information to auditors / frequent disputes with auditors, managers displaying significant disrespect for regulatory bodies, overly complex financial statements etc.);
- **transactional red flags** (involving certain transactions making no sense considering the company's operations, goals, and objectives, or an apparent or perceived override of internal controls in order to record the transaction etc.) and
- **documents related red flags** (like photocopied or missing documents, evidence of backdating of documents etc.). Please note that aforesaid instances of red flags are not exhaustive. Red flags appear in many different guises according to circumstances.
- **Other red flags** may include inappropriate or unusual journal entries, unexpected overdrafts or declines in cash balances, significant downsizing in a healthy market, frequent changes in auditors and sale of company's asset at under-market value / inventory shrinkage.

H

Whistle Blower Complaints and How to Deal with Them

Background and applicable Indian laws

A whistle blower ("**WB**") is a person who makes a 'disclosure'. A 'disclosure' means a concern, usually raised by an employee or group of employees of an organization or even a third party to the organization, in writing and in *bona fide*, which discloses information about a fraudulent, unethical or improper activity with respect to the organization and which is based on actual facts and is not speculative.

India's **Whistle Blowers protection act, 2014** (the "**WB Act**") was enacted with the intent to:

a. Receive complaints relating to disclosure of any allegation of corruption, wilful misuse of power / discretion against any 'public servant'

b. Inquire or cause an inquiry into such disclosure and

c. Provide adequate safeguards against victimization of complainant.

The WB Act is only applicable to corruption / bribery etc. Involving public servants. Till date, the provisions of the WB Act have not been notified in terms of section 1(3) of the WB Act.[39]

[39] Therefore, the WB Act cannot be said to be operational as on date.

Legal framework governing WB systems of listed companies

Section 177 of the Act read with rule 7 of Companies (Meetings of Board And Its Powers) Rules, 2014 (the "2014 rules")	If a company is either listed or accepts deposits from the public or has borrowed more than Rs. 50 crore from banks / public financial institutions, then such companies need to establish a 'vigil mechanism' / WB system to: (a) provide adequate safeguards against victimization of person using the WB system for reporting genuine concerns, (b) make provision for direct access to the chairperson of the audit committee (or the director appointed to play the role of audit committee) in exceptional cases, and (c) make disclosure of establishment of such WB system on the company's website and the board's report.
Rule 7 of the 2014 rules	In case of repeated frivolous complaints being filed by a director or an employee, the audit committee (or the director nominated to play the role of audit committee) may take suitable action against the director or the employee including reprimand.
Regulation 9a (6) of SEBI (Prohibition of Insider Trading) Regulations, 2015	This regulation mandated every listed company to make its employees aware of their WB system.
Regulation 4(2)(d)(iv) of SEBI (Listing Obligations and Disclosure Requirement) Regulations, 2015	Listed entities to comply with the corporate governance provisions like devising "an effective vigil mechanism/ whistle blower policy enabling stakeholders, including individual employees and their representative bodies, to freely communicate their concerns about illegal or unethical practices."
Regulation 22 of SEBI (Listing Obligations And Disclosure Requirement) Regulations, 2015	Regulation 22 of SEBI (LODR) Regulations, 2015 mandates listed companies to establish adequate safeguards in the vigil mechanism devised against victimization of the WB.
Regulation 30 of the SEBI (LODR) Regulations, 2015	Regulation 30 of SEBI (LODR) Regulations, 2015 mandates disclosure of all "material" event or information (including allegations dealt by WB system) to stock exchanges by listed companies
Companies (Auditor's Report) Order, 2020[40]	The Companies (Auditor's Report) Order, 2020 mandates companies to share information with the auditors, especially on WB complaints received during the year.

[40] Clause (xi), Fraud Reporting, Companies (Auditor's Report) Order, 2020. [4]

Legal framework governing WB systems of private companies

Presently, there is no statutory framework or specific WB law in force in India that governs the manner of dealing of WB complaints received by WB systems of private and unlisted companies. As a matter of practice, Indian private companies voluntarily incorporate a WB policy as part of extending their global policies. the 2020 India WB survey report of Deloitte[41] suggests that WB systems have increased employee confidence in the management and bolstered management sensitivity and intent to address fraud-related issues.

Effective WB system

In the Indian context, the 2020 India WB survey report of Deloitte also suggests that employee confidence in WB systems remains low. Considering the above, certain aspects that should be considered by any company seeking to establish an effective and adequate WB mechanism are:

a. **Reporting mechanism**: An effective WB policy should allow for meaningful, reliable, yet anonymised disclosures. Anonymity of the complaint is one of the quintessential factors that helps to lower the inhibition threshold for complainants. There should be a strong statement of support available on a company's website, to encourage employees to come forward and make necessary disclosures without any fear of adverse actions within the organisation or from the management.

b. **Complainant**: While many companies focus on providing a WB system primarily to their employees or group of employees, vital complaints are often raised by third parties (like business partners, vendors, customers, financial analysts, media etc.). Therefore, third parties should also be allowed to raise complaints.

c. **Effective evaluation and segregation**: Once a WB complaint is registered, the organization should evaluate it for its severity and should deal with it through its appropriate department. An organization's internal policy should factor in issues (for instance, performing a complete legal evaluation of its reporting and preserving obligations under the legislations that govern the company) while evaluating the nature of the complaint.

d. **Identified and transparent investigation**: The 2020 India WB survey report of Deloitte further suggests that majority of companies are not using any case management system to track and monitor all complaints received and communicate the ongoing status of any associated investigations.[42] companies should bear in mind that success of a WB

[41] Deloitte India Survey on the effectiveness of corporate whistleblowing mechanisms, available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-whistleblowing-survey-report-24june2020-noexp.pdf.

[42] Id.

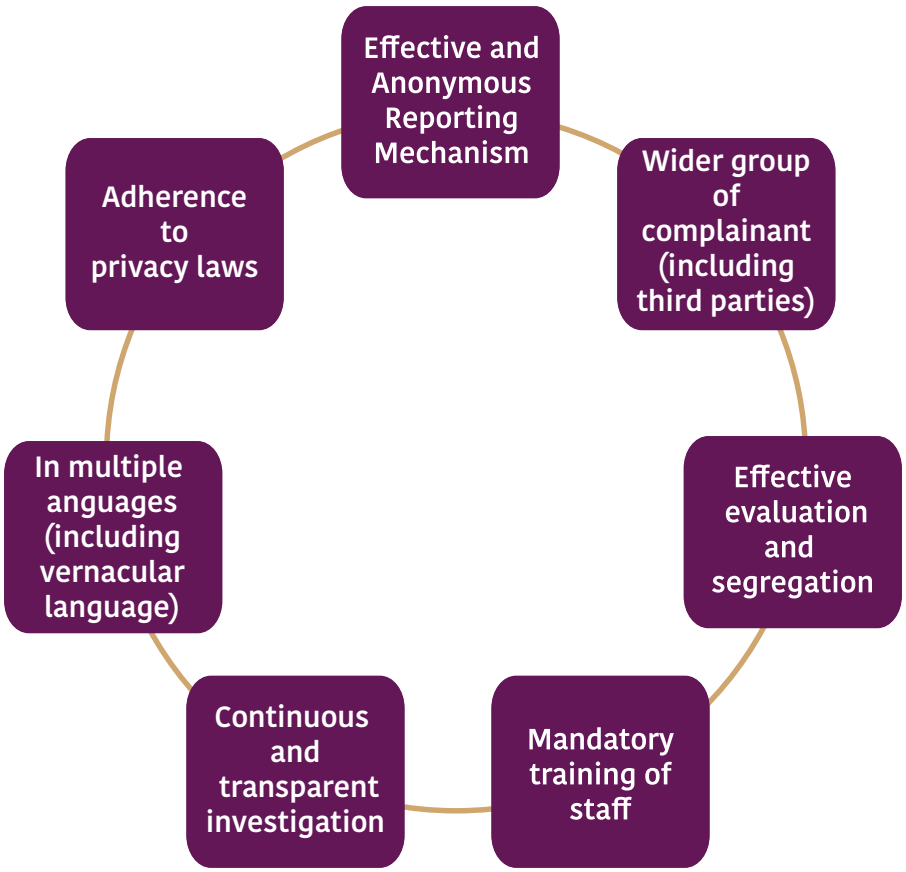
mechanism depends upon the perceived effectiveness of the mechanism by stakeholders. Hence, it is important that credible WB complaints are investigated by a team of independent personnel.independent personnel.

e. Language: A critical success factor for an effective vigil mechanism is its communication to employees, in more than one language, including the vernacular language of the place of residence of the employees of the company.

f. Privacy concerns: Adherence to privacy laws is a must while dealing with a WB complaint. At present, the information technology act 2000 and its corresponding information technology (reasonable security practices and procedures and sensitive personal data or information) rules 2011 mandate that body corporates that possess, deal or handle any sensitive personal data or information, are required to take consent of the information provider when (a) the data is collected/processed/reviewed; and (b) the data is shared / transferred to a third party. Further, companies should set out any potential cross border transfer to a foreign entity, in which case, the safeguards adopted by the foreign entity in protecting such data need to be understood as well.

g. A dedicate budget to ensure smooth functioning and wide coverage of the programme should be maintain by the company.

h. Lastly, the company should make provisions for mandatory annual training of staff and third parties on the programme.



Best practices for dealing with WB complaints

a. **Taking all complaints seriously**: Anonymous WB tips often include allegations that could, at first sight, seem baseless or vexatious. However, it is crucial for the WB team of a company to take every complaint seriously.

b. **Assessing the potential impact of a WB complaint**: The potential impact of a complaint on the company depends primarily on two factors: (i) the financial, legal, and reputational risk to the company; and (ii) the credibility of the complaint. Accordingly, a company should assess the potential impact of a WB company basis the aforesaid factor and determine whether to proceed with the investigation.

c. **Decision to investigate**: Depending on the information that the WB provides and its potential impact on the operations of the company, an evaluation as to whether the company needs to investigate the WB's concerns should be made. Sometimes, the alleged misconduct / issue is more of an hr issue than a legal breach / violation. The former can be referred to hr / another department of the company to follow up. In other instances, if it leads to a potential violation of the law / matter that could lead to civil or criminal liability for the company, the company should consider whether it needs to conduct an investigation into the allegations, using inside counsel or outside counsel, depending on the nature of the allegations.

d. **Developing an investigation plan**: Once a complaint is received and the decision is made to investigate, the in-house counsel of the company should lay out a plan, from start to finish, that will ensure the investigation will be thorough, efficient, objective and credible. Among other things, an investigation plan should lay out:

   i. *Scope of the investigation:* The scope of the investigation is influenced by several factors, such as criminal or civil exposure to the company (both domestically and globally), seriousness and nature of the allegations or possibility of shareholder litigation.

   ii. *Determining who will investigate the complaint*: The investigation plan should lay out the competent individual to investigate the complaint. If there's significant risk, the company should consider getting outside counsel involved. If that is not the case, the company can decide to handle the complaint internally, typically by human resources, compliance, or legal team. Further, to avoid conflict of interest, in cases where senior management / in-house counsel is implicated in the complaint, the company should generally engage outside counsel.

   iii. *Determining goals of the investigation*: The investigation plan should further lay out the objectives of the investigation.

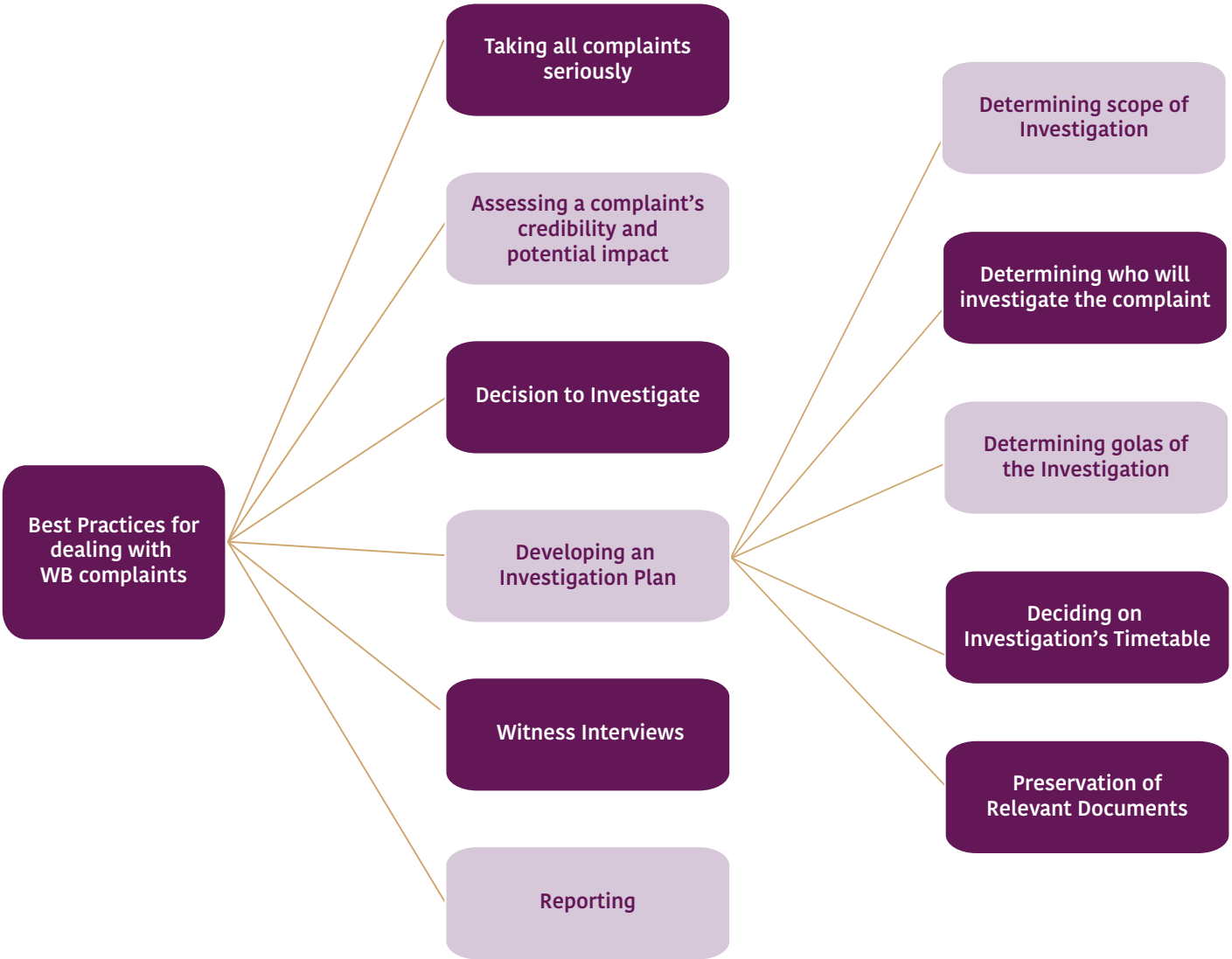
   iv. *Deciding on investigation's timetable*: It is crucial to form an opinion on the investigation timetable especially, if the company is facing an impending disclosure for

instance, disclosures made to a stock exchange under regulation 30 of the SEBI (LODR) Regulations, 2015 (as detailed above) or to the auditors under the Companies (Auditor's Report) Order, 2020.

v. *Preservation of relevant documents throughout the investigation*: It is quintessential to preserve the relevant documents throughout the investigation as they may be relevant during the evidentiary stage of the court proceedings.

e. **Witness interviews**: It is best to begin the process of witness interview early in the investigation to lock in the narrative and to prevent witnesses from being influenced.

f. **Reporting**: The final investigation report should follow a logical path that lays a basis for the conclusions the investigators make. Investigation reports must be tailored to the capabilities and culture of the company. Proposing unrealistic reforms may open the company up to future scrutiny by regulators. At the same time, investigators should be forthright in identifying changes the company should make to mitigate the issues examined.



I

Investigating Purported Fraud

Investigation sources

Fraud investigation resources generally fall into four categories / skill sets. In majority of the cases, most if not all of them are required to fully investigate a purported fraud. These are described below:

Investigative intelligence and analysis	⌝ Research component of the investigation. ⌝ Involves experts in publicly sourced information obtaining relevant information concerning individuals and entities suspected of involvement in the fraud.
Forensic accounting / transaction analysis	⌝ Forensic accountants are responsible for quantifying and evidencing identified fraudulent transactions.
Computer forensics	⌝ Involves the search, seizure and analysis of electronic evidence. ⌝ Rare for modern day frauds to be perpetrated without the involvement of computers.
Fieldwork and interviews / interrogations	⌝ First-hand sources to gather the information required to draw a conclusion. ⌝ Statements made during an interview can become admissible evidence, if obtained in an appropriate manner.

Conducting a fraud investigation

Every fraud incident is different, and responses will defer depending on the unique / specific circumstances of the concerned case. The following constitutes as a typical response if a fraud incident occurs, or suspicion of a fraud arises:

Investigative intelligence and analysis	⌝ Research component of the investigation. ⌝ Involves experts in publicly sourced information obtaining relevant information concerning individuals and entities suspected of involvement in the fraud.
Forensic accounting / transaction analysis	⌝ Forensic accountants are responsible for quantifying and evidencing identified fraudulent transactions. Discussed in detail in preceeding sections.
Computer forensics	⌝ Involves the search, seizure and analysis of electronic evidence. ⌝ Rare for modern day frauds to be perpetrated without the involvement of computers.
Fieldwork and interviews / interrogations	⌝ First-hand sources to gather the information required to draw a conclusion. ⌝ Statements made during an interview can become admissible evidence, if obtained in an appropriate manner.

Responses prior to initiation of investigation

a. **Assigning responsibility**: Responsibility of fraud investigation should be allocated on specific individuals. Those chosen to administer the role must come from appropriate legal and management level to authorise investigative actions and co-ordinate the organisation's overall response to fraud incidents.

b. **Receipt and initial assessment of suspicion / allegation / 'tip-off'**: Whatever be the source for initiation of fraud investigation (WB complaint / job change / audit / by accident etc.), certain actions should be taken in all cases. These include, *inter alia*, alerting the fraud incident manager that an allegation or suspicion exists; obtaining as much detail about the allegation as possible; the suspect should not be alerted that an allegation has been made throughout the investigation; maintaining a note of all actions/incidents that have happened since the information was received.

c. **Preparing accurate file notes of any conversations / correspondence which has occurred**. The investigative team should prepare precise notes of conversations or correspondences happening during the investigations. Such notes are relevant for court proceedings at a later stage.

At the conclusion of this stage, a decision must be made as to whether the allegation warrants investigation or is implausible or vexatious.

Responses during investigation

d. **Initial investigation**: Once a decision to investigate is made, an investigation plan or strategy must be prepared. This strategy will be dependent upon several circumstances, such as whether the suspect(s) are employees or outsider, whether the suspect(s) work in the premises, whether the alleged fraudulent activity is ongoing etc.

e. **Suspect interviews**: Suspect interviews should only be undertaken by skilled, experienced investigators. In most cases, they should only be conducted once all investigations are complete. Legal advice should be sought before interviews are conducted unless the investigative team is using trained, specialist investigators.

Responses post completion of investigation

a. **Reporting and subsequent actions:** Armed with evidence gathered through above exercises, the incident controller(s) / investigative team should obtain legal advice as to the appropriate way forward. Typical conclusions could include: (i) the evidence is insufficient or inconclusive, hence, no further action; (ii) the evidence is strong but requires further support, hence, continue investigations; or (ii) the evidence is conclusive. As per the conclusion reached, disciplinary action should be taken against the suspected employee.

b. **Legal actions**: The incident controller(s) / investigative team may also decide to take legal actions pursuant to the conclusion formed as detailed above. Legal actions may include injunctive reliefs against the suspect and civil action for recovery of defrauded funds, losses, and damages. Alternatively, the team may prefer to alert the police, in which case, the police decides whether to pursue it in the criminal side.

c. **Police referral**: On referring the fraud to the police, the police will usually proceed only once it has received sufficient evidence to support the allegations. Most fraud referrals are required to be 'assessed' by the police, as suitable for police investigation and prosecution. Therefore, the referrals should be made with proper evidence and proof.

d. **Personnel management and announcements**: this includes internal and external management of the incident after the investigation has been completed and legal or police action has been initiated. Rather than avoiding comment on the matter / relying on rumour, the organisation should clarify that the incident has been investigated, and that the matter has been reported to the police, in all of its internal and external announcements. The organization should also reassure the stakeholders about management's policy to pursue any and all such matters rigorously through the courts.

J

Understanding Fraud Measures in the Organizations

Background

The Price Waterhouse Coopers economic crime survey, which is adopted by Australian organisations, identified few basic fraud control and prevention techniques.[43] These techniques are used by organisations across the world to minimise the risk and impact of fraud and include: internal controls (94.2 percent), external audit (93.3 percent), ethical guidelines (87.5 percent), internal audit (86.5 percent), compliance program (78.8 percent), audit committee (76.9 percent), staff selection tests (75 percent), whistle blowing system (68.3), fraud risk management (64.4 percent), consultation on fraud prevention (53.8 percent), corporate security (52.9 percent) and information from publicly available sources (51 percent) etc.[44]

Some of the above-mentioned techniques have been discussed in the following paragraphs.

Fraud detection and prevention measures in the organisations

[43] PwC, Fraud – A guide to its prevention, detection and investigation, available at: https://www.pwc.com.au/consulting/assets/risk-controls/fraud-control-jul08.pdf.

[44] Id.

a. **Effective corporate governance mechanism and code of conduct**: The primary responsibility of fraud prevention and detection falls upon managers and board of directors. The presence of ethical policies / code of conduct make a positive contribution towards absence of fraud. It is essential to clearly define such policies to avoid fraudsters from exploiting the lack of clear guidelines and using them as an excuse for their actions. In their study, Jessup and Noblet observed that the common features of non-fraud firms include a strong management and qualified and active directors.[45]

b. **Internal audit**: Internal auditors are the first line of defence and have knowledge about the business environment and internal control structure. The detection of fraud in organisations is greatly dependent on internal auditors, to the extent that Deloitte found that 53 percent fraud cases were detected by internal audit in the Indian context.[46] It is advised that organisations refrain from outsourcing internal auditing and employ internal auditors permanently, thus helping set up a better internal control environment.

c. **External auditing:** Well-known fraud cases such as Satyam computers scam have revealed that fraud is exposed even when auditing is done by one of the big four audit firms. The Act requires auditors to report fraud or material misstatements to either the management or audit committee and the CG. ICAI has made it compulsory that external auditors provide reasonable assurance that the financial statement is free from any material misstatement, caused either due to an error or by fraud.[47]

d. **Whistle blowing policies.**

e. **Forensic accounting / auditing**: Forensic accounting and auditing improve the auditor's fraud detection abilities and act as a means for bridging audit expectation gap. It is therefore suggested that forensic accountants be given a participative role in preparation of the audit plan instead of a consultative role.

f. **Fraud risk assessment procedure**: Knowledge about fraud, identification of red flags and the participation of employees at all levels are the key requirements of fraud risk assessment. The express stipulation of risk assessment instructions plays an essential role in assessing the presence of fraud. Further, a formal approach is usually preferred over an ad-hoc approach for this assessment. Assessment must be made in accordance with the size, goal and complexity of the business and requires effective continuous updates. Updates to the assessment should be made considering all potential reasons that could lead to a fraud. The Deloitte 2020 survey highlighted that the key contributors to future

[45] Jessup, C. M., & Noblet, I. N. (2012), Fraud insight derived from stories of auditors of financial institutions. Journal of Forensic and Investigative Accounting, 4 (2), 206-243.

[46] Mangala, D., & Kumari, P. (2017), Auditors' Perceptions of the Effectiveness of Fraud Prevention and Detection Methods, IJCG, 10(2), 118–142.

[47] Mangala, D. & Kumari, P., Corporate Fraud Prevention and Detection: Revisiting the Literature (January 1, 2015), JCAR, Volume 4, Issue 1, January 2015, available at SSRN: https://ssrn.com/abstract=2678909.10(2), 118–142.

fraud were: limited understanding of new fraud risks which lead to gaps in the risk assessment and management procedures (19.78 percent), reliance on static, dated controls to prevent and detect fraud (14.39 percent), disproportionate access to information systems and decision making provided to a few individuals (12.95 percent) and unrealistic goals linked to monetary compensation (12.23 percent). Other factors include: inadequate due diligence on employees and third parties (8.63 percent), constraints on resources required to build a robust fraud risk management (7.55 percent), poor demonstration of ethical behaviour by the senior management (7.55 percent), lack of communication regarding fraud to employees (5.76 percent), unclear guidance about the changing business environment from regulatory authorities (4.68 percent), inadequate redressal of reported cases of fraud (4.32 percent) and inadequacy of channels to report suspicions (2.16 percent).

g. Reference check of employees / staff selection tests

h. Anti-fraud training of employees

i. Password protection and firewall: Passwords and firewalls are used to secure the access to internal information of the organisation from external parties, by placing hardware or software constraints between networks.

K

Considering Gaps in Internal Control Structure

Background

Research reveals that one of the key contributors in a case of fraud is poor internal control.[48] The strength of internal control in an organisation helps determine the extent of focus placed by auditors with a suspicious attitude over potential fraudulent acts. A strong internal control environment can be among the best methods for curtailing fraud if it is appropriately implemented through policies that are clearly written, well communicated and enforced in an effective and efficient manner. To ensure that internal controls remain effective, it is important to review and update them constantly, in accordance with the dynamic and fast changing business environment and technological processes.

Weaknesses in Internal Controls

a. **No Segregation of Duties**: Accounting responsibilities should not be accorded to just one person. Separation of duties is important to prevent giving a free pass to immoral employees to commit fraud, thus making the exercise of auditing redundant and equivalent to a lack of audit.

b. **Non-Systematic Record-Keeping**: Negative employee attitudes, poor execution of record management systems, insufficient training and low security of records are among the factors that lead to problems in record keeping. This deficient record-keeping eventually causes internal control breakdowns.

c. **Lack of Physical Access Control**: Physical access control ensures that the company's asset-related transactions are appropriately processed and that physical assets are properly secured from losses such as theft, underutilization, damage, errors and accidental destruction. Absence of such control exposes the organisation's assets to dangers from insiders as well as from foreigners.

d. Other weaknesses in internal controls of a company includes, *inter alia*, **lack of oversight, lack of audits and inappropriate transaction authorization**.

[48] Mangala, Deepa and Kumari, Pooja, Corporate Fraud Prevention and Detection: Revisiting the Literature (January 1, 2015). Journal of Commerce & Accounting Research, Volume 4, Issue 1, January 2015, pp 35-45, available at: https://ssrn.com/abstract=2678909.

How to Identify Gaps in Internal Control Structure?

a. **Cataloguing internal control procedures**: Cataloguing refers to the documentation of financial transactions, product designs and testing, purchase procedures, internal auditing etc. The next step in this process is to use this documentation to analyse and determine which parts of the company are prone to higher risk than others.

b. **Conducting a risk assessment**

c. **Conducting an internal audit**

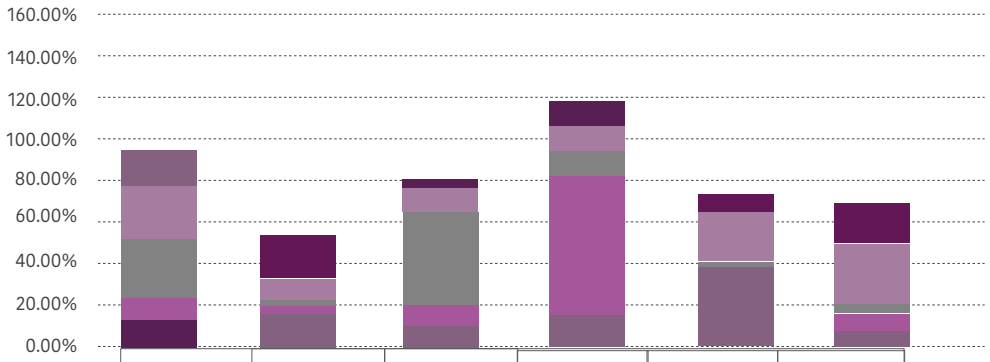
d. **Training and educating staff**

e. **Conducting regular inspections**

f. **Feedback from customers and stakeholders**

g. **Examining departmental reports**: This includes the examination of various areas of the company and identifying the ones that are not improving as expected or are becoming worse. These issues may be caused by other factors, but they may signal some type of internal control failure. The Deloitte 2020 fraud survey suggests that amongst the ecosystem players who could significantly improve fraud risk efforts in future, technology organisations can play a dominant role in fraud prevention, forensic experts and law enforcement in investigation, law firms in fraud response and anti-fraud education, and independent directors in fraud reporting. This has been represented in the chart below:

Deloitte 2020 fraud survey



	Fraud Prevention	Anti Fraud Education	Fraud Prediction	Fraud Investigation on	Other Fraud Response	Reporting Fraud
Law Enforcement Agencies	13.48%	17.98%	2.25%	37.08%	10.11%	19.10%
Independent Director	21.74%	9.78%	13.04%	6.52%	22.83%	26.09%
Technology Organisations	34.48%	2.30%	43.68%	10.34%	2.30%	6.90%
Forensic Experts	9.89%	1.10%	16.48%	69.23%		3.30%
Law Firms	11.83%	19.35%	4.30%	17.20%	38.71%	8.60%

L

Crisis Management

Background

Crisis Management is a risk management process that requires having the knowledge regarding the preparation for any crisis, maintaining a pro-active approach towards emergencies as opposed to a reactive one and responding with the correct response. It dramatically influences a company's chances of successfully navigating through a crisis. University of Melbourne's research depicts that 27 percent of the companies that have suffered a high profile crisis (refers to a crisis receiving a great deal of media attention) have had to shut their operations.[49] A successful crisis planning involves various steps as described below:[50]

Some of the above-mentioned techniques have been discussed in the following paragraphs.

a. **Understanding of Processes:** Before strategies for recovery and business procedures can be drafted, it is essential to understand the various processes that exist within the business. This also helps the organisation gain credibility with participants.

b. **Risk Assessments:** Risk assessment helps the company streamline its planning processes by focusing on high risk and high impact scenarios.

c. **Business Impact Analysis:** BIAs help by providing information regarding necessary processes and recovery time objectives, resource requirements and interdependency with other parties and processes.

d. **The Right Approach:** A structured methodology helps in guiding the conversation and uses the time of the participants in a more effective manner.

e. **The Right Amount of Time**: The time taken varies with respect to the complexity of the business unit. Therefore, prior knowledge of the business unit helps schedule the right amount of time.

f. **The Right People**: It is important to involve the right people to successful plan a crisis. There should be participation from the upper management for overall guidance as well as from the staff to help develop detailed recovery procedures.

---

[49] NSW Business Chamber, Crisis Management - How To Plan For The Unthinkable, International Institute of Directors and Managers, available at: https://www.iidmglobal.com/expert_talk/expert-talk-categories/finance-and-risk/disaster_plan/2_9_1551.html.

[50] Deloitte, Facing the Unknown: Crisis Management and the Role of Internal Audit (April 11, 2016), available at: https://na.eventscloud.com/file_uploads/6f0320514d6d17d3e83bab6f80e79ebf_CS2-1-FacingtheUnknownCrisisManagementandtheRoleofInternalAudit.pdf.

Core Crisis Management Issues

Establishing a crisis committee, agreeing on communication methods with members of that committee, assigning individual roles and responsibilities to those members and putting in contingency plans in place in the event of unavailability of such members is the first step towards crisis management. A clearly documented crisis management plan must be drawn up and communicated to the necessary people. This plan, however, should be flexible and should have the ability to change depending on the nature of the crisis.[51]

a. **Identifying the issue:** This will help the organisation identify the right set of people with the required skill set and experience, to help the company navigate through the crisis.

b. **Preservation of information:** The next step is to ensure that the all relevant data and information is preserved and consider whether there is a need to maintain privilege. Organisations should adopt as a rule of thumb to assume that privilege needs to be maintained and should therefore speak to their lawyers at an early stage.

c. **Stakeholder management and communications:** Communication needs to be maintained both internally and externally to keep control over the information and to avoid adding to the crisis. PR and communication must be part of every crisis management plan. The organisation should build its internal and external communications strategy crisis communication processes to alert stakeholders like staff, shareholders, government, industry, alliance partners and media.

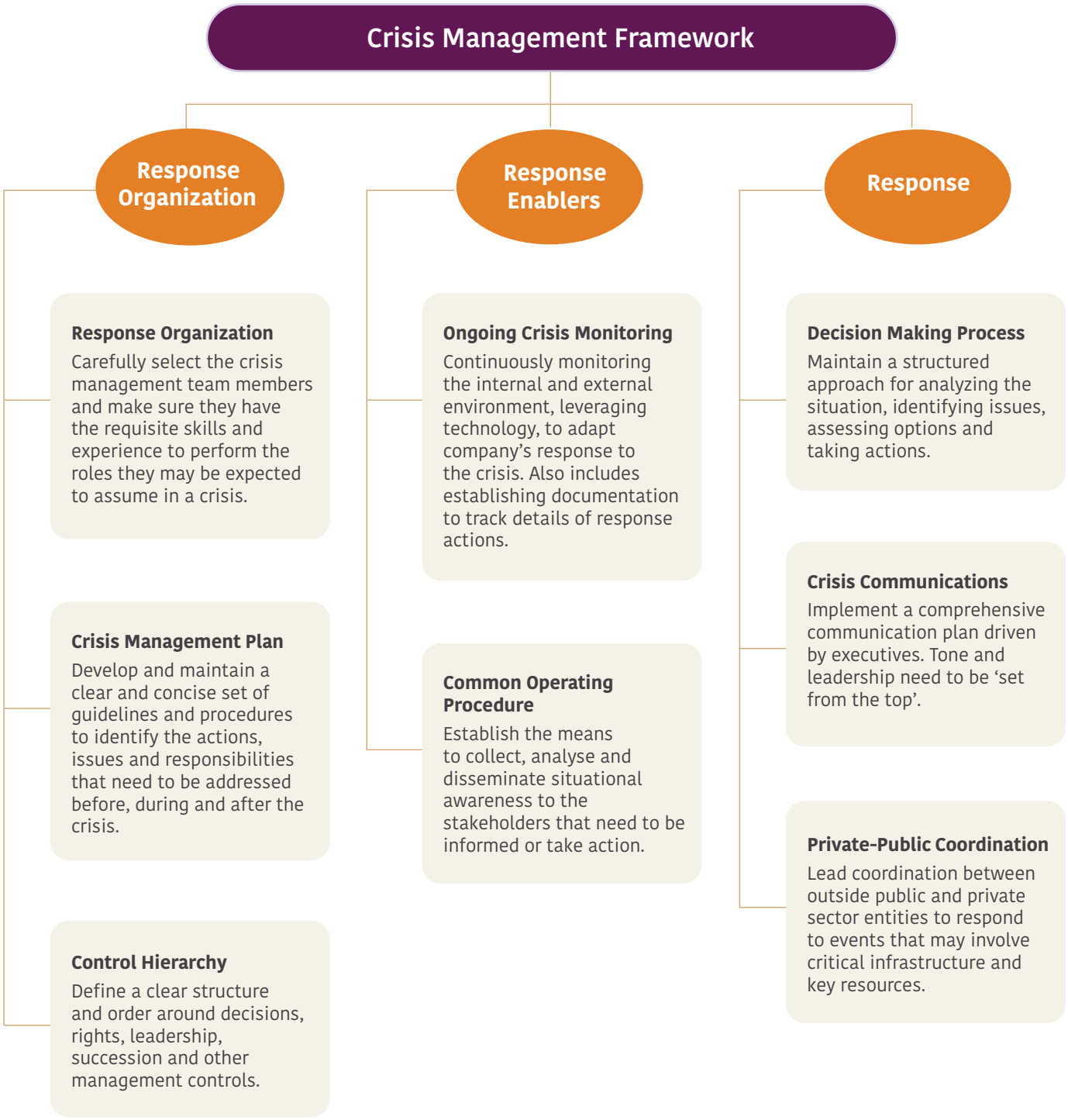
d. **External consultants:** Organisation must also make use of external crisis management consultants and corporate image specialists who can bring specialised expertise to the table.

e. **Flexibility in management of crisis:** Remaining flexible and nimble is key for any organisation in crisis. The committee should reflect on the objective and change it, if necessary.

f. **Learning from the crisis:** The organisation should take invaluable lessons from the crisis and must implement changes to ensure that they don't face any such crisis in the future.

[51] BDO LLP, 2020: A Fraudster's Perfect Vision for Fraud Opportunity? Why Crisis Management is Now More Important Than Ever, available at: https://iclg.com/practice-areas/business-crime-laws-and-regulations/3-2020-a-fraudster-s-perfect-vision-for-fraud-opportunity-why-crisis-management-is-now-more-important-than-ever.

The characteristics of an effective Crisis Management Program is illustrated below.



M

Legal Privilege and Investigations

The legal privilege or attorney-client privilege is often regarded as the crown jewel of the legal profession. It provides protection from disclosure of communications between a client and an attorney made for the purpose of seeking legal advice.

Legal professional privilege protects all communications between a professional legal advisor i.e. a solicitor, barrister or an attorney and their client from being disclosed without the express permission of the client. The privilege of protection is of the client and not that of the attorney. Legal privilege protects an individual's right to access justice by encouraging an open and complete discussion between an attorney and a client, who is not only shielded -from disclosing such communication but can also claim subsequent prejudice due to the disclosure.

The earliest known instance of the principle of legal privilege in English common law dates back to 1577, where in the case of *Berd vs. Lovelace*[52], where the court refused to compel the attorney to depose against his client. The position was further cemented in Greenough v. Gaskell[53] where lord brougham observed that in the absence of privilege, a client would not be able to fully disclose the facts to his attorney, which in turn would hinder his ability to seek legal advice.

What really is attorney work product?

The attorney work product is more inclusive than legal privilege. The work product doctrine states that an adverse party generally may not discover or compel disclosure of written or oral materials prepared by or for an attorney in the course of a legal representation, especially when prepared for the purpose of litigation.

Generally, there are two types of work product: opinion work product and ordinary work product. Opinion work product includes an attorney's mental observations, notes on key issues, and documents reflecting potential strategies. Ordinary work product includes information distinct from legal analysis, such as witness interview transcripts, reports of non-testifying experts and financial records from the client.

In the landmark case of *Hickman v. Taylor*[54], the US Supreme Court recognised the work product doctrine and held that the materials prepared by a party's attorneys in anticipation of litigation or for the purposes of litigation be protected from the scope of discovery under the federal rules of civil procedure. The US Supreme Court ruled that "*not even the most liberal of*

[52] Berd v. Lovelace, (1577) Cary 62.

[53] Greenough v. Gaskell, (1833) 39 ER 618.

[54] Hickman v Taylor, 329 US 495 (1947).

discovery theories can justify unwarranted inquiries into the files and the mental impressions of an attorney."

The legal position on work product doctrine in India is similar to the English law position. The Bombay High Court, in *Larsen & Toubro Ltd v Prime Displays (P.) Ltd.*[55], while deciding a petition for winding up filed by the respondents against the petitioner company, held in favour of the petitioner company that attorney-client work in anticipation of litigation is entitled to protection under sections 126 and 129 of the act. All documentation created (whether tangible or intangible) and communication between a client and an attorney in anticipation of litigation will be privileged communication, including any communication for the purpose of securing advice for the litigation; for obtaining or collecting evidence to be used in the litigation; and for obtaining information that will lead to such evidence, drafts of notices, pleadings and so forth, exchanged between the attorney and the client.

Information called for by the client and provided by an employee or a third-party agent, on the request of, and for the purpose of submission to, the attorney may also be protected.[56]

Unlike the legal privilege, which generally refers to communications between an attorney and a client, the work product doctrine often includes materials prepared by persons other than the attorney, as long as they were prepared for ongoing or potential litigation. This goes on to show that attorney work product doctrine covers a more comprehensive track than the legal privilege.

Legal position in India

Under the Indian Evidence Act, 1872 ("**the Evidence Act**"), any professional and confidential communication with the legal advisor is protected. Sections 126 to 129 of the Evidence Act codify the common law principles of privileged professional communication between an attorney and the client. It can be essentially summarised to say that any communication made for the purpose of seeking legal advice to an attorney would be protected. In India, any person who seeks an advice from a practicing advocate, registered under the Advocates Act, 1961, would have the benefit of the legal privilege and his/her communication would be protected under Section 126 of the Evidence Act. The Bombay High Court, in *Cecilia Fernandes v. State*[57], held that when considered in the light of the right of personal liberty given under Article 22(1) of the Constitution in order to be meaningful can be exercised only in confidence. The interpretation of the term 'legal privilege' in India is severely diluted, especially in terms of enforcement investigation wherein investigative agencies have accessed documents.

[55] Larsen & Toubro Ltd v Prime Displays (P) Ltd., [2003] 114 Comp Cas 141 (Bom).

[56] Woolley v North London Railway, (1868-1869) LR 4 CP 602.

[57] Cr. Misc. Application No. 9 of 2005, see also; Moti Bai v. State 1954, CriLJ 1591.

An attorney, without the express consent of the client, cannot disclose any communication made by the client, on behalf of such client; during the course of or for the purpose of his / her engagement as such attorney. Furthermore, an attorney cannot state the contents or conditions of any document he / she may have become acquainted with in the course of his/ her engagement as an attorney or disclose the advice provided to the client.

However, the privilege is subject to limitations, and the privilege shall no longer apply where disclosures are made with the express consent of the client, or where the communication is made in furtherance of any illegal purpose or where, post his/her engagement, the attorney discovers or observes a fact that a crime was committed or a fraud was perpetuated, it is immaterial whether or not the attention of the attorney was or was not directed to such fact by or on behalf of the client. Section 127 of the Evidence Act expands the scope of privilege provided under Section 126 by imposing a similar duty on interpreters, clerks and servants of the legal adviser.

Section 128 of the Evidence Act provides that the attorney cannot disclose any information which is deemed privileged under section 126 unless the client calls upon the legal adviser as a witness and questions him on the same.

Furthermore, Section 129 of the Evidence Act lays down that no one shall be compelled to disclose to the court any confidential communication which has taken place between him and his legal professional advisor, unless he offers himself as a witness. In this case, the attorney may be compelled to disclose any communication as deemed necessary by the court to explain any evidence so provided by the attorney, but no other. The Calcutta High Court, in *Sudha Sindhu v. Emperor (AIR 1935) Cal 101*, held that all communications between an accused person or indeed any litigant and his legal advisors are privileged and confidential.

Courts have further clarified on the issue of legal privilege by holding, *inter alia*, that to claim privilege under Section 126 of the Evidence Act, a communication by a party to his/her pleader must be of a confidential nature.[58] However, privilege does not apply to communications made before the creation of a relationship of a pleader and client.[59]

In addition to the provisions under the Evidence Act, professional communication between a legal advisor and a client is accorded protected status under the Advocates Act, 1961 and the Bar Council of India rules (the "**BCI Rules**"). The BCI Rules, under Rule 17, Chapter II, Part VI, stipulate that '*an advocate shall not, directly or indirectly, commit a breach of the obligations imposed by Section 126 of the Evidence Act*.' In addition to this, Rules 7 and 15 of the BCI Rules on an advocate's duty towards the client state that communication between the client and the attorney cannot be disclosed by the attorney, in any manner whatsoever, and that an advocate should not take advantage or abuse a client's confidence.[60] A violation of these rules would subject the attorney to disciplinary proceedings.

[58] Memon Hajee Haroon Mohomed v. Abdul Karim, [1878] 3 Bom. 91.

[59] Kalikumar Pal v. Rajkumar Pal, 1931 (58) Cal 1379, Para 5.

[60] The Bar Council of India, Rules on Professional Standards, Rule 7 and Rule 15, available at http://www.barcouncilof-india.org/about/professional-standards/rules-on-professional-standards/.

With respect to an in-house counsel, the legal position was clarified by the Supreme Court in *Satish Kumar Sharma v. Bar Council of Himachal Pradesh*[61], wherein, the Supreme Court held that "*if a full-time employee is not pleading on behalf of his employer, or if terms of employment are such that he does not have to act or plead but is required to do other kinds of functions, then he ceases to be an advocate. The latter is then a mere employee of the government or the body corporate*". The judgment also referred to Rule 49, Section VII, Chapter II, Part VI of the BCI Rules, stating that "*an advocate shall not be a full-time salaried employee of any person, government, firm, corporation or concern, so long as he continues to practice and shall, on taking up any such employment intimate the fact to the bar council on whose roll his name appears, and shall thereupon cease to practice as an advocate so long as he continues in such employment. An advocate cannot be a full-time salaried employee. The only exception is if the person is a law officer of the Central Government of a state or of any public corporation entitled to be enrolled in the bar.*"

In *Municipal Corporation of Greater Bombay v. Vijay metal works*[62], the court held that "*a salaried employee who advises his employer on all legal questions and also other legal matters would get the same protection as others, viz., barrister, attorney, pleader or vakil, under sections 126 and 129, and, therefore, any communication made in confidence to him by his employer seeking his legal advice or by him to his employer giving legal advice should get the protections of sections 126 and 129*." Thus, in India, in order to qualify as privileged, the communications between clients and in-house attorneys would have to be tested on the touchstone of whether the in-house counsel is a full-time salaried employee as contemplated under Rule 49, Section VII, Chapter II, Part VI of BCI Rules. Further, the issue of whether the advice sought is in legal or executive capacity would also be a key distinguishing factor.

Privilege during internal investigations

Internal investigations pose a great challenge in terms of preserving legal privilege due to their sheer size and involvement of a wide nature of non-legal parties. The objective of an internal investigation is to understand the scope of the issue, remediate the problem, and to formulate a suitable response to regulators, government authorities or investigative agencies in one's own or a foreign jurisdiction, as the case may be. In terms of investigation, maintaining privilege is crucial and it is important to structure and conduct the internal investigation in a manner that maximises the legal privilege available in a particular jurisdiction. It is imperative to note that legal privilege in many jurisdictions across the globe may not recognise communications with an in-house counsel, as protected by attorney-client privilege.

It is advisable for corporations or clients in the process of commencing an internal

[61] AIR 2001 SC 509.

[62] AIR 1982 Bom 6.

investigation to engage an external attorney or law firm at the outset and ensure that the investigation is carried out at the direction of the attorney. It is recommended to create and preserve written records demonstrating the purpose of the investigation and the legal advice sought in connection with anticipated litigation, if any. The records must reflect that key decision-makers at the company are within the client group so that there is no ambiguity in relation to applicability of privilege to the communication between the client and the attorney.

While creating written reports of the investigation or witness interviews, the distinction between ordinary work product and opinion work product must be kept in mind. It would be wise to consider whether the written reports will be protected under the privilege laws in each jurisdiction where the company can face potential litigation or enforcement actions. Furthermore, it is prudent to ensure that all non-legal advisers are retained or supervised by counsel overseeing the investigation.

The company as well as the attorney must take steps to avoid inadvertent waiver by ensuring the investigation and any related documents or reports are treated as confidential and not disclosed outside the investigation team.

Preserving and protecting privilege: best practices

Privilege applies only to communications where an attorney's role was primarily for the purpose of rendering legal advice or assistance. While determining applicability of privilege, the following factors are deemed relevant:

a. The context of the communication and the content of the document;Preservation of information

b. Whether the legal purpose permeates the document and can be separated from the rest of the document; and

c. Whether legal advice is specifically requested and the extent of the recipient list.

d. Best practices in the age of zoom

Furthermore, to determine legal professional privilege between in-house counsel and corporate employees, courts have adopted two methods: one, the control group test, and two, the subject matter test. Under the first approach, communication from individuals outside the control group (i.e. The officers authorised to seek legal advice or control the legal affairs of a company) is not protected. Under the subject matter test, privilege is limited to communication from corporate employees for the specific purpose of securing legal advice for the corporation. Communication with an in-house counsel in relation to business as opposed to legal advice may not be protected by privilege.

In a recent decision, the UK Court of Appeal confirmed that legal advice privilege is also subject to a 'dominant purpose' test. In doing so, the court has confirmed that legal advice and litigation privilege are two limbs of the same privilege, and similar considerations apply.[63]

[63] The Civil Aviation Authority v Jet2.Com Ltd, R. (on the Application of Jet2.com Limited), [2020] EWCA Civ 35.

Simply put, for legal advice privilege to apply, the dominant purpose of a communication must be to obtain, or give, legal advice.

In a recent decision, the UK Court of Appeal confirmed that legal advice privilege is also subject to a 'dominant purpose' test. In doing so, the court has confirmed that legal advice and litigation privilege are two limbs of the same privilege, and similar considerations apply. Simply put, for legal advice privilege to apply, the dominant purpose of a communication must be to obtain, or give, legal advice.

Many communications are presumed privileged, such as those in which "attorneys are examining and commenting upon a legal instrument, like a patent application, contract for a study, or the retention of experts." In view of this, it is recommended that:

i. While seeking legal advice, it must be clarified at the outset that the communication is for the dominant purpose of "seeking legal advice" or "for the purpose of providing legal advice", as such statements assist in substantiating claims of legal professional privilege.

ii. Irrespective of the platform or mode, while providing legal advice to a client, attorneys must document the communication as "legal privileged" and provide legal support for any advice provided.

iii. It is advisable to clarify that any non-legal business issues or documents are provided or discussed separately, and purpose of the said communication is to seek or provide legal advice.

iv. Where the client is a large organisation or company with legal and non-legal staff, the presence of non-legal staff or those outside the control group on attorney communications may undermine the privilege. Therefore, it is advisable to limit access of such communication only to those legal and non-legal team members with a direct connection to the legal matter at issue.

v. In addition to this, labelling the communication with "do not forward" and instructing the team involved to limit circulation of a communication is recommended.

It is highly recommended that companies while conducting internal investigations should strive to protect the privilege at the outset so as to retain the flexibility to decide later whether and to what extent a privilege waiver is advisable. An internal investigation structured to maximise legal privilege will allow the company greater control over how and when to disclose the relevant information.

ANNEXURE – A

A. Indian Contract Act, 1872

Section 17 of the Indian Contract Act, 1872 states:

"fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto of his agent, or to induce him to enter into the contract:

1. *The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;*
2. *The active concealment of a fact by one having knowledge or belief of the fact;*
3. *A promise made without any intention of performing it;*
4. *Any other act fitted to deceive;*
5. *Any such act or omission as the law specially declares to be fraudulent.*

Explanation.—mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak, or unless his silence is, in itself, equivalent to speech.

B. Report of the working group on electronic banking

In the context of electronic channel-based frauds, the definition of 'fraud' was suggested in the report of the study group on large value bank frauds set up by the RBI in 1997 in the following manner:

"a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank."[64]

[64] Report of the Working Group on Electronic Banking, Chapter-6, Cyber Fraud, available at: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111_C6.pdf.

ANNEXURE – B

The following table includes some important sections that attract liability u/s 447 of the Act.

Section	Fraud with respect to	Who will be penalised
7(5)	Registration of a company	A person furnishing false information or suppressing any material information of which he or she is aware
8	Affairs of the company being conducted fraudulently	Every officer of the company who is in default.
34	Misstatement in prospectus	Every person who authorizes issue of prospectus
36	Inducing persons to invest money	The person doing so
38	Personation for acquisition etc. Of securities	Any person who does so
46(5)	Issuance of duplicate certificate of shares	Every officer of the company who is in default.
75(1)	Acceptance of deposit with intent to defraud depositors or for any fraudulent purpose	Every officer of the company who accepted the deposit.
206(4)	Conducting business of a company for a fraudulent or unlawful purpose	Every officer of the company who is in default.
213	Other cases: A) business of a company being conducted with intent to defraud its creditors B) fraud, misfeasance, or other misconduct of the company or any of its members C) company withholding information from members with respect to its affairs, which they may reasonably expect	Every officer of the company who is in default and the person(s) concerned in the formation of the company or management of its affairs.

251(1)	Application for removal of name from register with the object of evading liabilities/intent to deceive	Persons in charge of management of the company.
266	If tribunal concludes that an employee during the period of his employment with a company was guilty of any misfeasance, malfeasance or non-feasance in relation to the sick company	Any person who is found so guilty
339(3)	Conducting business of company with intent to defraud its creditors, any other persons or for any fraudulent purpose	Every person who was knowingly a party to the business in the aforesaid manner.
448	Making a false statement in any return, report, certificate, financial statement, prospectus, statement, or other document required by or for the purpose of any of the provisions of this act or the rules made thereunder	Person making such a statement etc.

Notes

Contributors

Faraz Alam Sagar
Partner
faraz.sagar@cyrilshroff.com

Pragati Sharma
Principal Associate
pragati.sharma@cyrilshroff.com

Kishan Kumar Gupta
Associate
kishankumar.gupta@cyrilshroff.com

Offices of Cyril Amarchand Mangaldas

Mumbai

Peninsula Chambers,
Peninsula Corporate Park,
GK Marg, Lower Parel,
Mumbai – 400 013, India
T +91 22 2496 4455
F +91 22 2496 3666
E cam.mumbai@cyrilshroff.com

Delhi-NCR

Level 1 & 2, Max Towers,
C-001/A, Sector 16 B,
Noida – 201 301,
Uttar Pradesh, India
T +91 120 669 9000
F +91 120 669 9009
E cam.delhi@cyrilshroff.com

Bengaluru

3rd Floor, Prestige Falcon Tower,
19, Brunton Road, Off M G Road,
Bengaluru – 560 025, India
T +91 80 6792 2000
E cam.bengaluru@cyrilshroff.com

Ahmedabad

Shapath - V 1304/1305,
Opposite Karnavati Club, S G Road
Ahmedabad – 380 051, India
T +91 79 4903 9900
F +91 79 4903 9999
E cam.ahmedabad@cyrilshroff.com

GIFT City

Cyril Amarchand Mangaldas – OFC,
415, Pragya Tower, GIFT City,
Gandhinagar - 382 355, Gujarat, India
T +91 79 4903 9900 F +91 79 4903 9999
E cam.giftcity@cyrilshroff.com

Singapore

61 Robinson Road,
#11-03, Singapore - 068893
T +65 63292260
E cam.singapore@cyrilshroff.com
(CAM Singapore Pte Ltd., UEN: 202137213R)

presence also in hyderabad and chennai


BANK
Credit card protection
FRAUD PREVENTION
Data protection
Cybersecurity
Identity protection


FRAUD ALERT
CONFIRM
Click here for more information