



FORENSIC

India Fraud Survey Report 2010

ADVISORY

Foreword

With greed increasingly informing the thought process and the actions of a large number of persons, fraud has a bigger presence in our lives than ever before. Fraud, an intentional deception made for personal gains or to damage another individual, is a significant factor worldwide in today's competitive world, and in entities irrespective of their size. Fraud is a major source of risk which can have disastrous effects on the finances of a company. It can cause irreversible and often irreparable damage to the image and reputation of a company. In recent times, with increase in awareness, companies have started focusing on pro-active risk management strategies. However, a lot remains to be done, especially having regard to the complexity of instruments and the speed of transactions.

India has had its share of frauds and their incidence has often significantly impacted investor confidence. In an atmosphere of doubt and disbelief financial statements are often viewed with scepticism. This has also led to erosion of confidence and reduced trust among participants in the financial system.

The KPMG India Survey Report 2010 is an effort to provide a clear picture of what really happens in corporates today. The findings are, to put it mildly, disquieting. The mistrust of employees towards their senior management is unmistakable. Despite this, control mechanisms are not in place in most organisations and hence, the need for risk mitigating strategies is unquestionable. It is time that India Inc. sits up and ends its tolerance of unethical behaviour, bribery and corruption. Managements of companies have not only to act ethically but also to intensify their efforts to protect their companies from fraud. They should develop pro-active risk management mechanisms that can anticipate, prevent, understand, detect and respond to fraud.

This report highlights the urgent need for action from managements of companies against fraud. Even a strong regulatory system cannot always prevent fraud. The key lies in management decisions and recommendations to establish formal control systems that can help prevent or at least deal with fraud. I am hopeful that this survey will not only enhance awareness but also persuade corporates to move faster on the road to fraud prevention and risk mitigation.



M. Damodaran

Advisory Board Member
Audit Committee Institute
KPMG in India

Amongst words that were often heard or read in the media during 2009 like 'credit crisis', and 'recession', 'fraud' also featured prominently, especially in the Indian media.

Regulatory activities, the economic downturn of 2009 and recent corporate frauds have all combined to impact the perceptions of fraud levels in India. Outsourcing, increase in the use of third parties and technology have combined to open up new avenues of frauds like e-crime and Intellectual Property (IP) theft. These developments have intensified the debate on the readiness of Indian companies to effectively deal with fraud and the importance that companies assign to fraud risk management.

The investor community and stakeholders now expect company boards and audit committees to take the onus of proactively monitoring their companies' efforts to understand and mitigate fraud risks. Non-executive directors are expected to play a major role in challenging management on the adequacy of their fraud risk identification and mitigation plans.

In such a scenario, it is useful to analyse the extant and extent of fraud and fraud risk management practices in corporate India.

KPMG's Forensic practice in India has been undertaking the India Fraud Survey once every two years since 1995 to provide India Inc. with insights into the degree of fraud awareness, nature of fraud risks, trends in fraudulent activities, and the required mitigation strategies.

The survey questionnaire was published as an e-survey in Jan 2010 and sent out to close to 1000 leading organisations in India. The survey respondents include Chairman/ Managing Directors, Chief Financial Officers, Heads of Internal Audit and Compliance, Fraud Risk Managers and other senior management personnel across various industry segments.

We take this opportunity to express our gratitude to the people and organisations who took time to respond to the survey. The report and its findings would have been unaccomplished without the support of the respondents and all of those who made this survey possible.

We hope that you will find this survey insightful.



Richard Rekhy
Head of Advisory
KPMG in India



Deepankar Sanwalka
Head of Forensic Services
KPMG in India

Executive Summary

There is a rise in the incidence of fraud – ineffective control systems and diminishing ethical values are key contributors to this trend

An overwhelming majority of the respondents indicated that the incidence of fraud, overall and specifically within their industry and company, is rising thereby indicating that India Inc needs to deal with fraud risks firmly. Supply chain fraud (procurement, distribution and revenue leakage) is the single most exposed area. Weak internal control systems, eroding ethical values and a reluctance on the part of the line managers to take decisive action against the perpetrators are cited as the most vital underlying reasons for frauds being on the rise.

75%

Fraud in corporate India is on the rise.

54%

Fraud is on the rise within their industry.

45%

Fraud (suspected and actual) has increased within their organisations.

Stakeholders view financial statement frauds as one of the major concerns in India

Stakeholders in India continue to perceive financial statement fraud as a major area of concern. A desire to achieve / exceed targets and earnings of senior executives linked to financial performance are the reasons for senior management involvement in such frauds. Ineffective whistle-blowing systems, lack of objective and independent internal audit functions with forensic skills, inadequate oversight of senior management activities by the audit committee and weak regulatory environment are the reasons for growing worries in respect of financial statement fraud.

81%

Financial statement fraud is a major issue.

63%

Desire to meet / exceed market expectations the most significant reason to commit financial statement fraud.

62%

Disagree that strict disciplinary actions are imposed for cases involving financial statement fraud.

Fraud risk management is not prevalent in India Inc.

Indian companies have a reactive approach to dealing with fraud. Even amongst those that do undertake a fraud risk assessment, the focus is more on financial frauds rather than a holistic assessment. The usage of data analysis tools to analyse critical patterns and trends in data and understanding scenarios of potential fraud which should be inter-woven into the fraud risk assessment process is still work in progress. Respondents suggest that a fraud risk management program should be a shared responsibility across the company board, senior management, internal audit and risk functions.

41%

Do not have a formal fraud risk management framework.

60%

Usage of technology tools in detecting trends and anomalies in data is average to poor.

58%

Data analytics are either not used or only partially used.

The enemy within continues to pose the biggest threat

Committing frauds is not confined to a select few, both junior and senior employees are perpetrators of frauds. The quantum of fraud in value terms is also increasing. The encouraging sign is that fraud detection mechanisms have improved with a majority of the frauds being detected through internal audits and whistle-blower mechanisms rather than by accident (as indicated in our 2008 Fraud Survey). However, the incidence of legal action against fraudsters is low with a majority of the frauds being investigated and dealt with internally.

75%

All fraudulent activities, except Intellectual Property (IP) fraud were perpetrated by employees.

47%

Frauds are unearthed by internal audits.

35%

Legal action initiated against the fraudster.

Bribery and corruption continue to remain a challenge in conducting business

Bribery and corruption is viewed as an inevitable aspect of doing business in India. Bribery and corruption are most rampant in seeking routine regulatory approvals and to win new business from prospective clients. Despite the presence of anti-corruption laws, weak regulatory enforcement has contributed to the current impasse. With Indian companies going global, we see an increasing trend of Indian companies pro-actively taking measures to adhere to international anti-bribery laws/ regulations (e.g.: Foreign Corrupt Practices Act) and strengthening their code of business ethics at the board and senior management levels to regulate dealings with external stakeholders.

37%

Bribes are mostly paid to get routine administrative approvals from Government.

38%

Bribery an integral feature of industry practices.

56%

Tone at the top critical to combat bribery and corruption.

Intellectual Property, computer-related fraud, bribery and corruption and supply chain fraud are going to be the risk areas in coming years

Whilst supply chain and bribery and corruption will continue to dominate the fraud horizon, Intellectual Property and e-crime are emerging as the new dimensions and organisations in India seem ill equipped to fight these threats. Strong enforcement of Intellectual Property and anti piracy laws, the right to audit within third party contractual arrangements, vendor compliance / performance reviews and technology preparedness through document management and retrieval systems are important focus areas if organisations have to successfully counter these new types of fraud threats.

53%

e-commerce and computer related fraud are the biggest threats going forward.

62%

IP laws are poorly enforced.

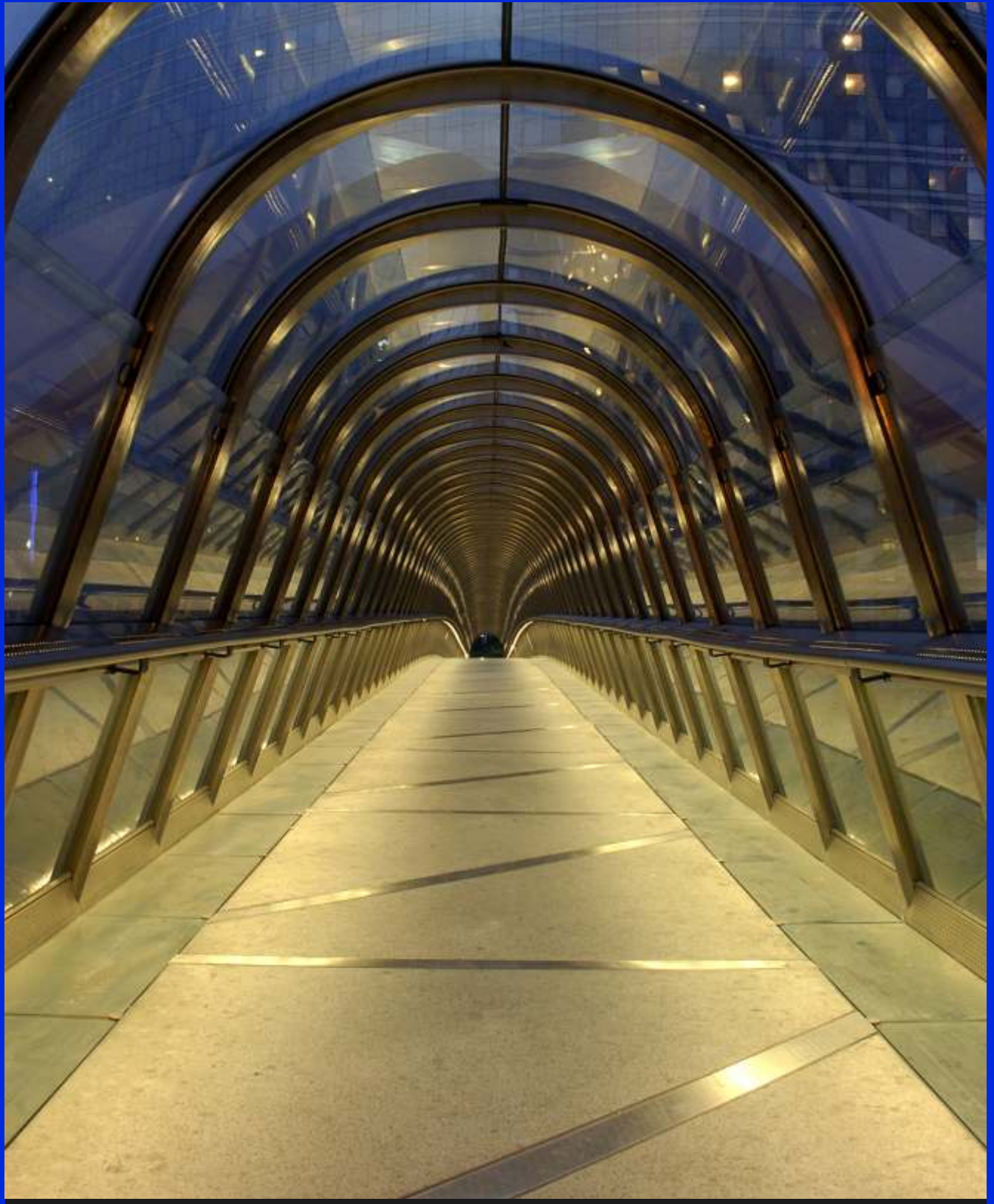


Table of contents

Perception of fraud in India	01
Fraud is on the rise	01
Financial statement fraud continues to be a major concern	02
Processes vulnerable to fraud	05
Factors contributing to an increase in frauds	05
Feeling the pain: Fraud experience in organisations	09
Nature and perpetrators of fraud	09
Value of frauds	12
Fraud detection and response	12
Getting the house in order: Fighting the menace	15
Strengthening corporate governance	15
Fraud risk management	18
Shades of things to come	25
Bribery and corruption	25
Intellectual Property fraud	29
E-crime	31
Supply chain fraud	32
Conclusion	36
Profile of respondents	37



Perception of fraud in India

Volatile economic conditions coupled with increasing business and technological complexities have led to increased opportunities for fraud. Organisations have to constantly deal with fraud and compliance challenges in today's business environment. Not surprisingly, a majority of the survey respondents perceive an increase in the level of fraud in India, in general, and also within their industry.

Fraud is on the rise

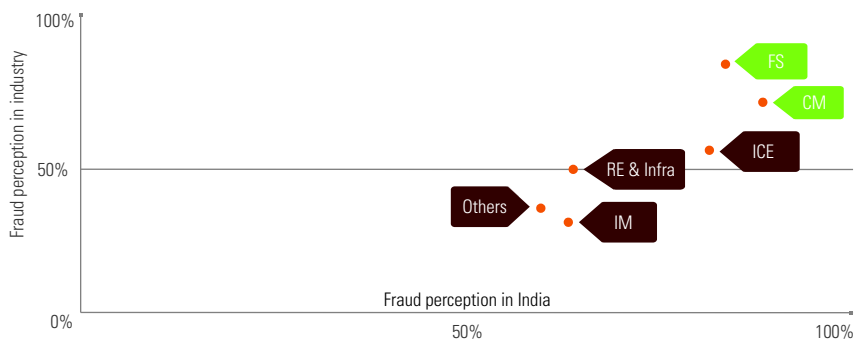
Seventy five percent of the respondents believe that fraud incidences in India have increased in the last two years, however, only 54 percent believe that fraud incidences have increased in their industry. Further, 45 percent of the respondents believe that fraudulent activities have increased in their organisation, again suggesting a rising trend in white-collar crime.

An industry-wise analysis of responses reveals that respondents from Financial Services and Consumer Markets industry segments perceive the level of fraudulent activities to be significantly high in India and their respective industry.

75%

fraud incidences in India have increased in the last two years

Figure 1: Perceptions of fraud



FS - Financial Services CM - Consumer Markets RE - Real Estate and Infrastructure
IM - Industrial Markets ICE - Information, Communication and Entertainment

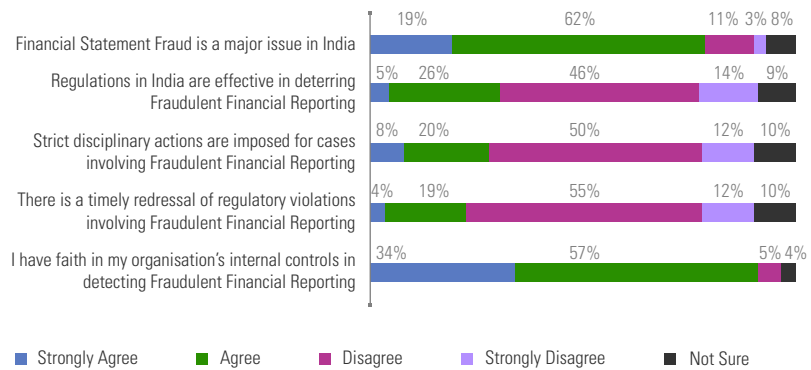
Source: KPMG in India's Fraud Survey 2010

Breakup of these industry segments is given in the profile of the respondents

Financial statement fraud continues to be a major concern

Considering the current economic environment, 81 percent of the respondents perceive financial statement fraud as a major issue in India. Over 60 percent of the respondents believe that enforcement of regulations and regulatory environment are inadequate in dealing with financial statement fraud.

Figure 2: Perceptions of financial statement fraud



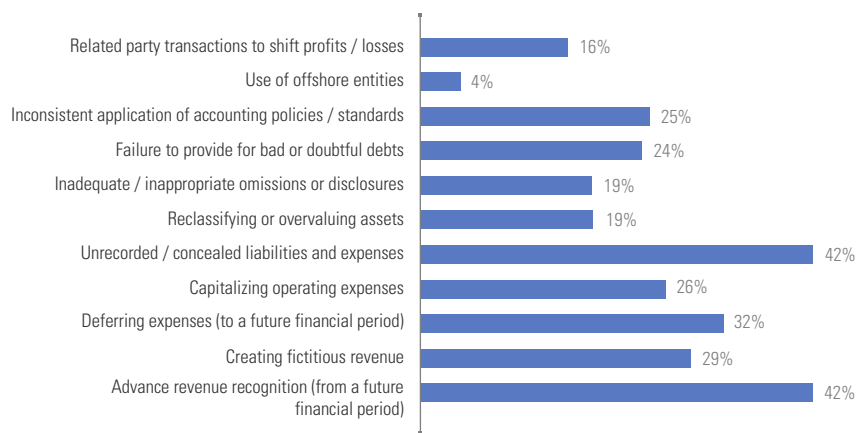
Source: KPMG in India's Fraud Survey 2010

In a recessionary environment, cost reduction initiatives increase the potential for internal control breakdowns and frauds, especially financial statement fraud. Therefore, with emerging signs of economic recovery, it becomes imperative for companies to re-evaluate their cost reduction initiatives. Companies should consider whether the cost reduction initiatives will stand the test of time, especially, once the economy turns back to growth.

Forms of financial statement fraud

Typically, financial statement frauds take the form of manipulation of critical accounts such as revenue, capital expenses etc. 'Advance revenue recognition' and 'Unrecorded/ concealed liabilities and expenses' are the most common forms of financial statement fraud (42 percent each).

Figure 3: Common forms of financial statement manipulations (multiple choice)



Source: KPMG in India's Fraud Survey 2010

“It is more harmful than any financial misappropriation when the head honcho manipulates organisational objectives on a continuous basis to suit personal agendas and beliefs.”

President of a Publishing House

Contributing factors

As for the motive of resorting to the aforementioned forms of manipulation, 63 percent respondents indicate pursuit of meeting market expectations and 61 percent respondents indicate performance based remuneration as the main reasons. Further, 66 percent respondents identify management override of controls as a key factor that facilitates the occurrence of financial statement fraud.

Reasons for financial statement fraud

63%

pursuit of meeting market expectations

61%

performance based remuneration

Figure 4: Reasons behind financial statement fraud (multiple choice)

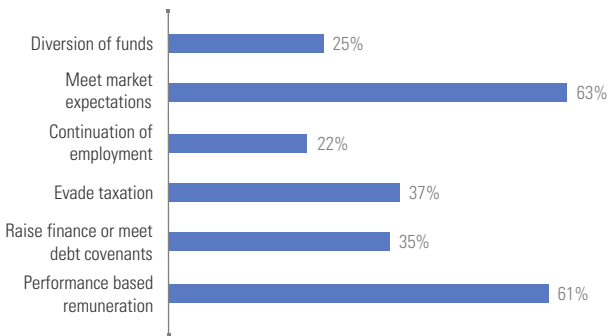
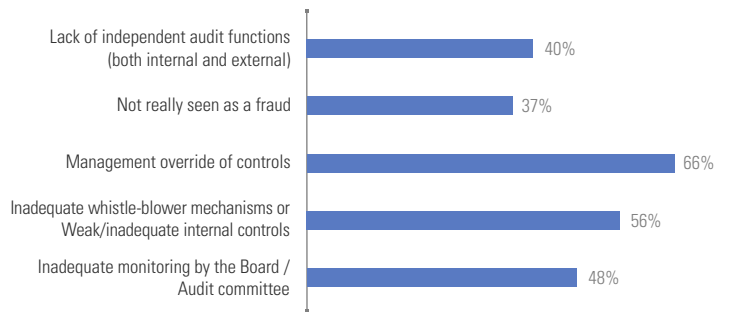


Figure 5: Factors facilitating financial statement fraud (multiple choice)



Source: KPMG in India's Fraud Survey 2010



Combating financial statement fraud

The damages caused by accounts manipulation can be severe and invariably spread far wider than the organisation concerned. The Satyam case last year sharply brought into focus the impact that a financial statement fraud can inflict on a company and its stakeholders.

Drivers, risk areas and red flags

From our experience on various engagements related to financial statement fraud, the following key issues have emerged:

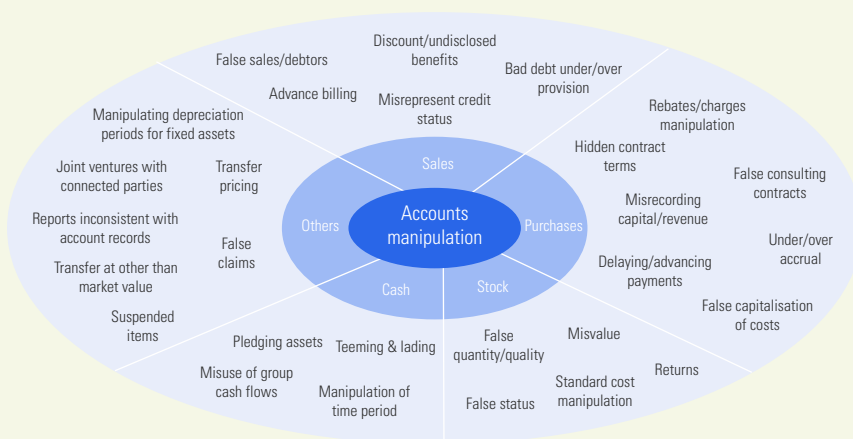
- Financial statement fraud is often orchestrated by senior management and usually involves a group rather than an individual. Motivation at this level can be varied, and is usually more complex than simply financial gain, it could include anything from pressures to report "favourable" results or enhance share price value to enhancing performance based incentives.
- Experience gained by KPMG Forensic through assisting clients, as well as our observation of other reported events has taught us that certain items within the financial statements are especially prone to manipulation. These, together with the forms that the manipulation can take, are illustrated in the Figure below.

- An alarming increase in the use of falsified documentation to give a semblance of legitimacy to fraudulent transactions has been observed. Perpetration of fraud in this manner makes detection immensely difficult during regular audits or management reviews, unless these are focussed forensic reviews.

Warning signs are usually present in the financial information of a subsidiary, division, joint venture or a group, and can sometimes be woefully evident on hindsight. While the precise signs are dependent on the sector or industry in which the organisation operates, some generic indicators include:

- items within the profit and loss account are based on judgment rather than hard data.;
- high levels of manual journals and accruals without automatic adjustment;
- Unusual fluctuations in sales or forward purchase orders, particularly around the year end;
- reported results are consistently in line with the budget; and
- Profits do not appear to be converted into cash, etc.

Common forms of accounts manipulation

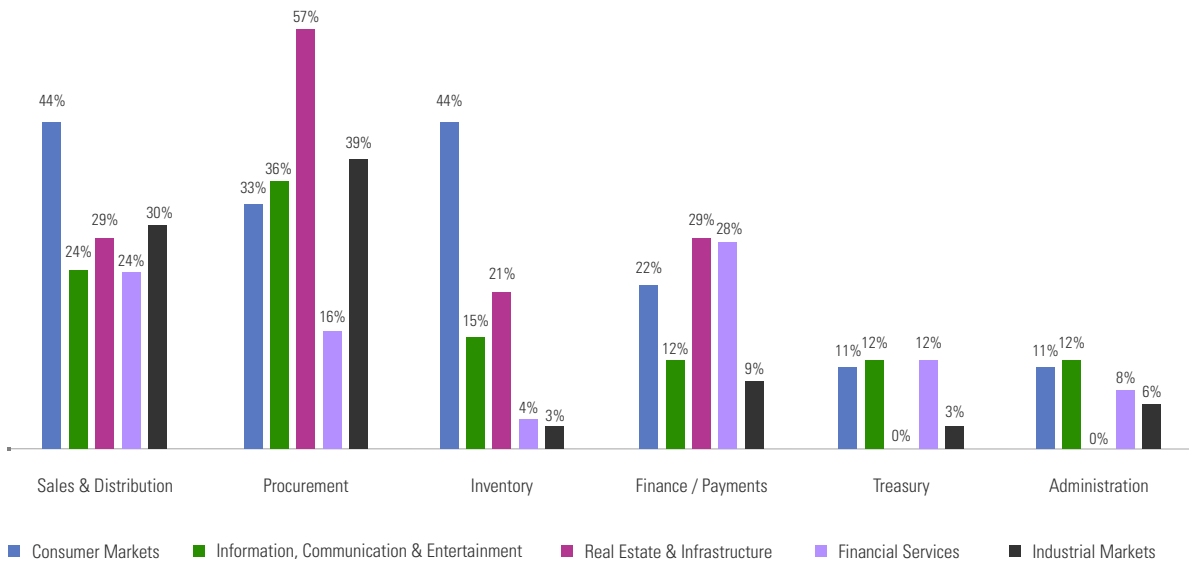


Though there is more interest and awareness around financial statement fraud amongst audit committees and company managements, there are deficiencies in instituting appropriate prevention, detection and response mechanisms. Going forward, we do expect lot many companies to proactively use and invest in technology, institute focussed fraud risk management exercises and encourage transparency in internal and external financial reporting to effectively respond to the growing menace of financial statement fraud.

Processes vulnerable to fraud

Our survey results indicate 'Procurement' and 'Sales and Distribution' to be the most vulnerable processes across industries. Notably, 57 percent of the respondents from real estate and government industry segment rate 'Procurement' as high risk while 44 percent of the respondents from consumer markets industry segment rate 'sales and distribution' as high. Interestingly, respondents perceive lower levels of risk in 'Finance and Payments', 'Treasury' and 'Administration' functions.

Figure 6: Processes perceived as most vulnerable to fraud risks (multiple choice)



Source: KPMG in India's Fraud Survey 2010

Factors contributing to an increase in frauds

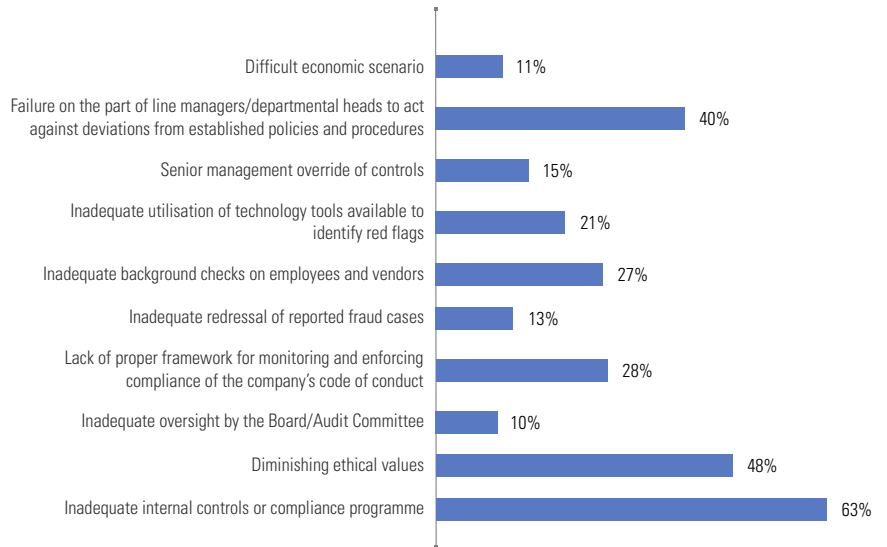
An effective control framework is essential to help minimise the risk of fraud. In fact, survey respondents indicate weaknesses in the control framework as a major factor for the occurrence of fraud.

Similar to our 2008 Fraud survey, 63 percent identify inadequate internal controls/ compliance program as a key contributing factor. Additionally, a combination of diminishing ethical values (48 percent) and a failure on the part of line managers / departmental heads to act against deviations (40 percent) from established policies and processes were cited as reasons for the increase in instances of fraud.

63%

Inadequate internal controls/ compliance program is a key contributing factor to increase in frauds

Figure 7: Factors contributing to an increase in fraud (multiple choice)



“At times, operating management may interpret red flags differently or ignore them completely”

Head of Internal Audit of a large conglomerate

Source: KPMG in India's Fraud Survey 2010



Why internal controls fail to prevent frauds?

Internal controls that address fraud risk could reside across different layers of the organisation's hierarchy, making it important to ensure that there is proper alignment between multiple levels.

Typically, from our experience, the following are some of the key reasons for ineffectiveness of internal controls:

- The lack of clarity in assigning ownership for internal controls – for instance compliance teams becoming responsible for financial controls result in control responsibilities not being embedded within the business.
- Inadequate oversight of the control environment in times of change and lack of alignment of the organisational roles to the configuration of roles (IT rights) within the IT systems. For instance, in implementing IT systems, certain individuals are assigned super user rights in the initial part of the implementation and these rights are not appropriately monitored/ revoked post implementation.
- Failure to implement early warning indicators or continuous monitoring processes i.e. through usage of data analysis tools to identify trends and inconsistencies in data sets, which can provide a holistic evaluation of the control deficiencies, the underlying root causes and their potential impact.
- The lack of periodic assessment of the effectiveness of supervisory controls (i.e. controls that monitor the operation of other controls such as an effective internal audit function) to minimise the potential for management override of controls.

Companies where the internal audit reports functionally to the audit committee and not to the CEO/ CFO have stronger anti-fraud monitoring mechanisms. In these organisations, the audit committee plays a key role in explicitly approving the audit plan including the scope, coverage, skill sets and tools used to audit fraud risk areas and the results of these assessments.







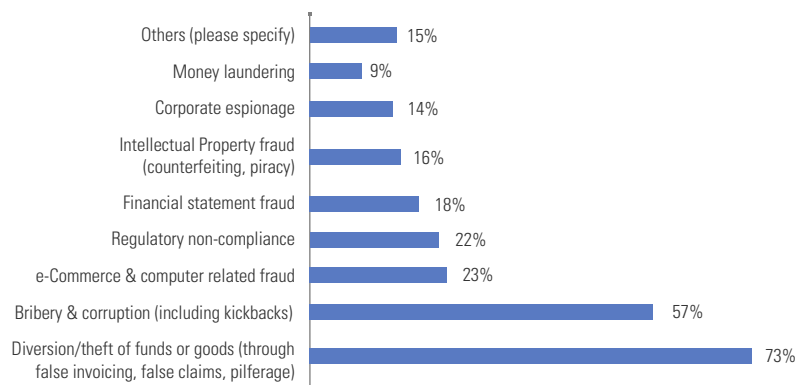
Feeling the pain: Fraud experience in organisations

The threat of fraud looms large, no matter the size of the company. The value, type and frequency of fraud vary based on several factors such as the effectiveness of internal controls, the degree to which responsibilities are devolved and complexity of automated systems and processes. However, whatever be the type of fraud, internal parties (management and non management employees) tend to have a higher propensity to commit fraudulent activities than external parties (customer, vendor or business associate).

Nature and perpetrators of fraud

As indicated previously, 45 percent of the respondents indicate that they have experienced fraud in their organisation over the last two years. Majority of the respondents have experienced theft of funds/ goods and bribery and corruption (including kickbacks). Specifically, while 73 percent of the respondents indicate that they have experienced diversion/ theft of funds/ goods (through false invoicing, false claims, and pilferage), 57 percent indicate that they have experienced bribery and corruption related fraud. Among other types of fraud, e-commerce and computer-related fraud was experienced by 23 percent of the respondents.

Figure 8 a: Types of fraud experienced by respondents (multiple choice)



Source: KPMG in India's Fraud Survey 2010

73%

Have experienced diversion/ theft of funds/ goods as the most common fraud in their organisation

A profiling of the fraud perpetrators in the respondent organisations reveals that over 75 percent of all fraudulent activities, except Intellectual Property (IP) fraud were perpetrated by employees, reaffirming that the 'Enemy within' poses the highest risk.

Further, among employees, non-management employees are perceived to pose higher risks than management employees. Over 50 percent of the respondents indicate that non-management employees were involved in most of the fraudulent activities. However, financial statement fraud and regulatory non-compliance are typically attributed to the management cadre.

External parties such as customers, vendors and business associates are perceived to pose the highest risk in areas such as e-commerce and computer-related fraud, bribery and corruption and IP fraud.

Figure 8 b: Key fraud perpetrators (multiple choice)



Source: KPMG in India's Fraud Survey 2010

“There is an increasing trend of the customer, outside elements and bank staff colluding together to commit frauds resulting in investigation of frauds all the more difficult without the help of enforcement authorities”

Senior Vice President Compliance of an Indian Bank

“Ethics and Values need to be driven strongly with appropriate rewards and recognition”

Head of Compliance of a leading IT firm

'Enemy within' – Why employees are one of the key perpetrators of frauds?

Employee fraud is not uncommon these days. The trend from the survey report clearly depicts that employees have caused significant damage to the organisations by committing fraud. At this juncture we need to understand four critical aspects relating to employee fraud.

Why an employee commits a fraud?

An employee often commits fraud because of four key reasons, namely, greed, financial stress, dissatisfaction with the employer/managers or just to experience the thrill of surpassing critical controls.

For instance, in a case investigated by us, an employee having an authority to issue international money card for employees traveling abroad, outstripped the controls, camouflaged the documentations, authorised international money card in the name of multiple employees and transferred funds from such cards to his personal bank account.

However, the employee had not utilised the money transferred to his account. During an enquiry, he revealed that he enjoyed the thrill of breaking the controls.

Why is it easier for an employee to commit fraud?

An employee by virtue of his/her position is aware of the processes and internal controls within the organisation. Therefore, it becomes easier for him to circumvent controls. For instance, an employee in the procurement department was well aware of the process that required him to obtain a minimum of three quotations for any purchases. He, in connivance with a vendor created two fake quotations and passed the procurement transaction at more than reasonable rate to the vendor for kickbacks.

In our view, undisclosed conflict of interest with vendors/ suppliers/ contractors, is one of the key frauds committed by employees.

Why it does not get noticed?

Often when it comes to fraud, organisations are in denial and critical red flags may be ignored on the pretext that these are isolated instances. Also, ethical employees ideally should have nothing to fear from whistle-blowing. However, in reality, whistle-blowing is not always perceived to be an independent and painless/undemanding mechanism. The whistle-blower may feel insecure and choose to remain silent, especially in cases where a senior member of the organisation or a known member is involved in fraudulent activities. Despite the efforts of organisations in establishing the ethical culture within, the social barrier is a phenomenon that needs to be addressed. Moreover, as employees are the part of system it is easier for them to camouflage the fraud.

What are common red flags/ indicators of an employee's involvement in fraudulent activities?

The common warning signs that may indicate potential fraud by an employee are marked by:

- personality changes
- late working hours
- reluctance to take leave
- sudden change in lifestyle
- cuts corners or bends rules
- does not produce supportive documents etc.

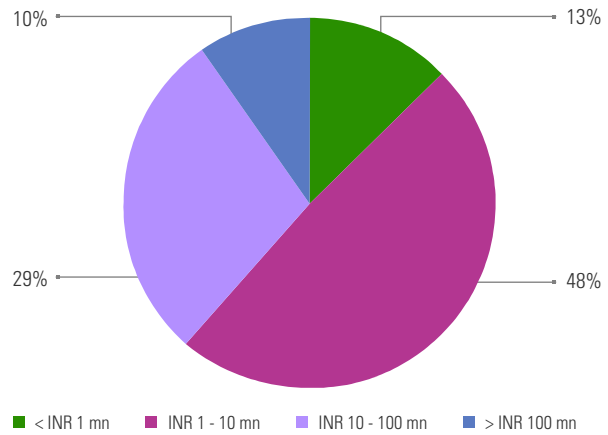
Value of frauds

The perception of India Inc that fraudulent activities are on the rise in India in last two years is not unfounded. The survey results indicate that the quantum of frauds has increased manifold over our 2008 Fraud survey. 87 percent of survey respondents state that their organisation had incurred fraud losses of more than INR 1 million as against 47 percent in our last survey.

87%

fraud losses more than INR 1 million

Figure 9: Value of fraud

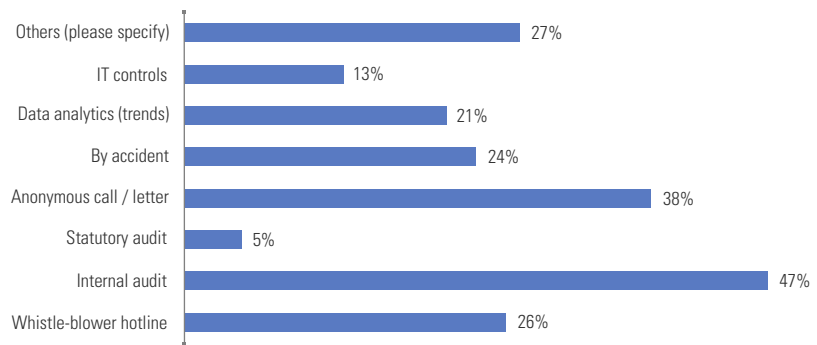


Source: KPMG in India's Fraud Survey 2010

Fraud detection and response

In the past, our surveys have revealed that most of the fraudulent activities were detected by accident. With the change in the corporate culture and organisational control framework, we believe that the trend in detection of frauds has changed for the better. True to this belief, 47 percent indicated that fraud incidents in their organisation were detected through internal audit. Further, 26 percent indicate whistle-blower mechanism as a means for detecting fraud, and 38 percent indicating anonymous calls/ letters.

Figure 10: Mode of fraud detection (multiple choice)



Source: KPMG in India's Fraud Survey 2010

Others include: vendor complaints, background verification, etc.

The detection mechanism reflects the organisation's fraud control mechanism, ethics, culture and tolerance to fraud. An effective framework to detect fraud involves an independent and empowered internal audit and risk functions and a well publicised and documented whistle-blower mechanism. Once fraud is detected, organisations should respond appropriately and initiate remedial action to undo the damage, to the extent possible.

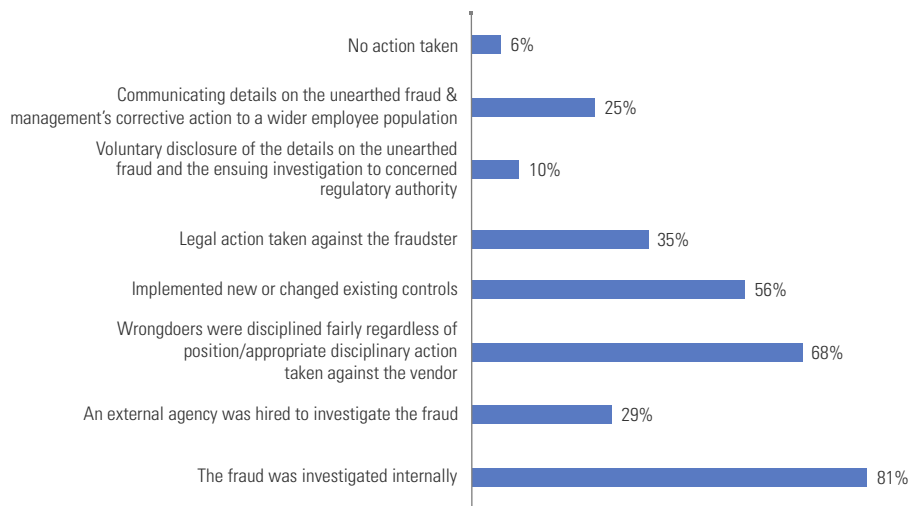
Only **35%** of the respondents initiated legal action against the fraudster

Majority of the survey respondents indicate that upon detection, their companies respond by initiating an internal investigation and disciplinary action. Specifically, 81 percent of the respondent organisations initiated an internal investigation and 68 percent initiated disciplinary action against the perpetrators. However, only 35 percent respondent organisations initiated legal actions against the fraudsters. Typically, companies refrain from taking legal action and prefer separating the fraudsters (employees and external parties).

Action taken by organisations greatly depends upon their outlook and tolerance towards fraud as well as their appetite to deal with law enforcement and legal channels.



Figure 11: Corrective action steps adopted (multiple choice)



Source: KPMG in India's Fraud Survey 2010







Getting the house in order: Fighting the menace

The key to preventing fraud is to understand the ways in which it can affect a company, and introduce controls to recognise and prevent it from occurring. Strong governance practices and a structured Fraud risk management process assists organisations in identifying and addressing potential fraud risks that could have a major impact on the company. Proactive detection and mitigation of the fraud risks inherent to business processes are integral components of an effective Fraud risk management program.

Strengthening corporate governance

Companies should create a broad program that manages and integrates fraud prevention, detection and response efforts. Responsibilities of managing such a program should be shared across the company board, senior management, internal audit and risk functions.

The company board along with the audit committee constitutes a critical component of the company's fraud risk management program. An independent and empowered board/audit committee goes a long way in strengthening the fraud risk management framework.

In response to a question on board independence, an overwhelming 95 percent of the respondents indicate that they are reasonably sure of the independence of their board of directors. Further, 92 percent indicate that their board/audit committee reviews and discusses issues raised during the organisation's fraud and misconduct risk assessment. Additionally, 86 percent indicate that their board/audit committee reviews and discusses with internal and external auditors the quality of the organisation's antifraud programs and controls.

On the issue of whistle-blower mechanism, 77 percent of the respondents indicate that their board/audit committee reviews the functioning of this mechanism or a similar mechanism.

Typically, respondents segregate Fraud risk management responsibilities as follows:

- Prevention: The responsibility of prevention is primarily with the board, along with C' suite officers.
- Detection: The responsibility of detection is primarily with internal auditors and the risk and compliance head.
- Investigation: The responsibility of investigation is with internal auditors and risk and compliance head.

Figure 12: Responsibility on Fraud risk management

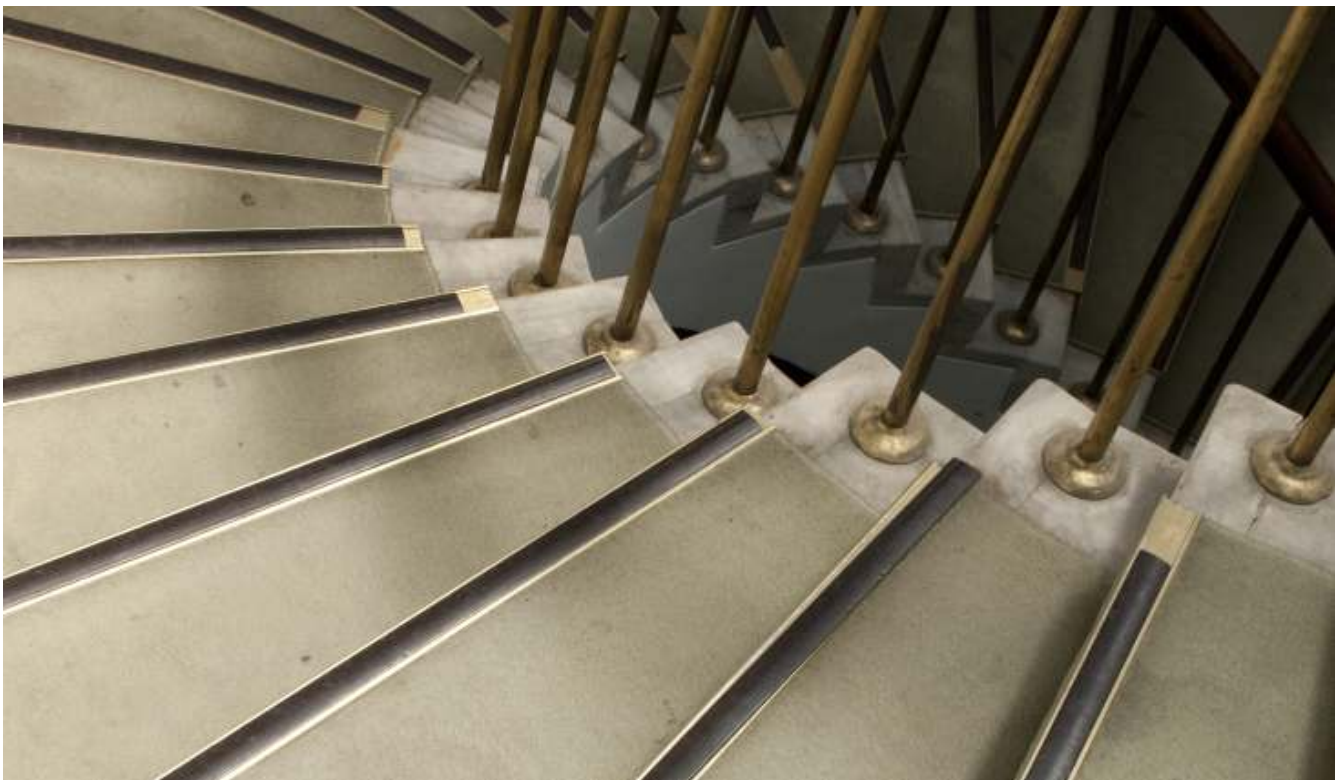
	Prevention*	Detection*	Investigation*
Board	●	○	○
Audit Committee	◐	◑	◑
CEO/Managing Director	◐	◑	○
Chief Financial Officer	◐	◑	◑
Risk & Compliance Head	◐	◑	◑
Chief Security Officer	◑	◑	◑
Internal Auditors	◑	◐	◑
External Auditors	○	◑	◑

Source: KPMG in India's Fraud Survey 2010

*Degree of responsibility depicted by 'Harvey Balls' based on score: 95-100: 1; 75-94: ¾; 50-74: ½; 25-49: ¼; < 25: 0. Score indicates the percentage of survey respondents highlighting degree of responsibility for fraud risk management across various levels.

"A well defined ethics policy, open channels of communication and strong internal control systems are important to minimise fraud in an organisation."

Vineet Kapur - Chief Financial Office, Carrier India



Strengthening corporate governance to combat fraud effectively – A three pronged strategy adopted by leading organisations

Enhance the effectiveness of the audit committee

- Explicitly review and approve the appointment of auditors and the audit plans for adequacy of scope, coverage and performance.
- Proactively monitor major financial transactions, choice of accounting policies and compensation policies including coordination with other board committees.
- Conduct 'in camera' executive sessions with internal and external auditors separately without the management being present.
- Review and approve anti fraud programs and controls.
- Scrutinise related-party transactions closely including seeking independent advice from experts.

Establish an effective anti-fraud program

- Putting in place a formal program for identification, assessment and monitoring of fraud risk areas.
- Review of the internal and external audit assurance plans to assess how they address fraud risk areas.
- Review the organisation's tools and techniques to combat fraud (data analytics, key performance indicators, segregation of duties).
- Review the organisation's approach to investigate fraud and

suspected instances of fraud including the adequacy of the reporting process.

Establish an objective and independent internal audit function

- Establish reporting lines of the Chief Internal Auditor to the Audit Committee and not management.
- Help ensure that internal audit teams undertake process reviews of key strategic projects / new operations to identify control weaknesses / fraud risks.
- Help ensure that as far as practicable financial/ operational and IT audits are seamlessly combined so as to help ensure that the IT implications of operational controls are appropriately assessed.
- Help ensure that internal audit undertakes ethical audits to assess the importance given to ethics and how ethical violations are dealt with.
- Review the skill sets present within internal audit to effectively audit fraud risk areas (knowledge of the business, forensic skill sets, seniority within the organisation and ability to leverage technology).

Fraud risk management

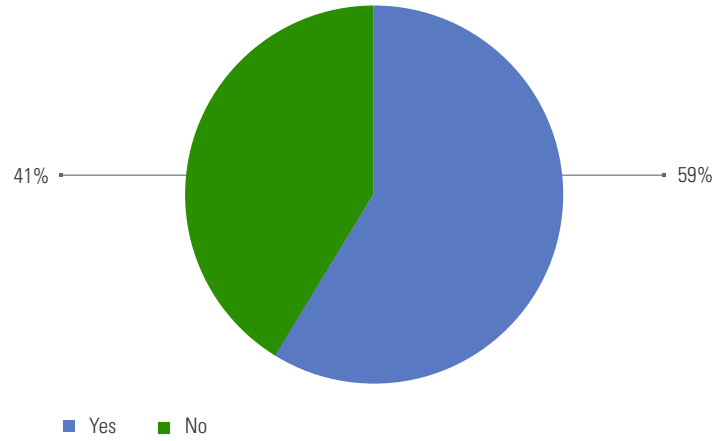
Forty one percent of the respondents indicate that their organisations do not have a formal Fraud risk management framework. Perhaps because of the buoyant regional economies, management of fraud risk was not hitherto at the top of the agenda. The increase in frauds and adverse reputation consequences that come in its wake makes it imperative that organisations adopt a proactive approach to fraud risk management.

41%

do not have a formal fraud risk management framework

Though the respondents perceived that their organisations had effective board oversight of fraud risks, it has to be considered in light of the fact that only 59 percent of the respondent organisations undertake a formal fraud risk assessment exercise.

Figure 13: Fraud risk management framework in organisations



Source: KPMG in India's Fraud Survey 2010



Fraud risk management

A comprehensive assessment of fraud risks, is essential for the management to gain knowledge on critical risk factors and deploy appropriate controls to avoid losses.

Why is fraud risk management essential?

- Many organisations are geared to deal with fraud in a reactive manner, in that they are not aware of the various ways in which fraud can occur. These companies fail to understand that the price they may have to pay for a fraud is significantly higher than the cost of a robust anti-fraud mechanism
- Often, the tsunami of fraud, leads to significant loss of market capitalisation, loss of a talent pool built and nurtured over years, loss of clients gained and grown over decades, and in some instances, also threatens the very existence of the organisation
- Many fraudsters always test the controls framework with insignificant values and basic fraud schemes to start with, to see if their frauds are detected, before they move on to larger values and more sophisticated schemes of

committing fraud. This highlights the importance of appropriate corrective action and the way in which it could greatly reduce future fraud risks.

Fraud risk management: A broad-based approach

An effective, business-driven fraud and misconduct risk management approach is one that is focused on three objectives:

- Prevention: controls designed to reduce the risk of fraud and misconduct from occurring in the first place
- Detection: controls designed to discover fraud and misconduct when it occurs
- Response: controls designed to take corrective action and remedy the harm caused by fraud or misconduct

Prevention	Detection	Response
Board/audit committee oversight		
Executive and line management functions		Internal audit, compliance and monitoring functions
<ul style="list-style-type: none"> • Fraud and misconduct risk assessment • Code of conduct and related standards • Employee and third-party due diligence • Communication and training • Process-specific fraud risk controls 	<ul style="list-style-type: none"> • Hotlines and whistle-blower • Auditing and monitoring • Proactive forensic data analysis 	<ul style="list-style-type: none"> • Internal investigations protocols • Enforcement and accountability protocols • Disclosure protocols • Remedial action protocols

Mitigating factors adopted by companies

While establishing controls to assist in timely detection of fraudulent activities and taking corrective action is essential, it is equally important for companies to establish controls to reduce the risk of fraud and prevent it from occurring in the first place.

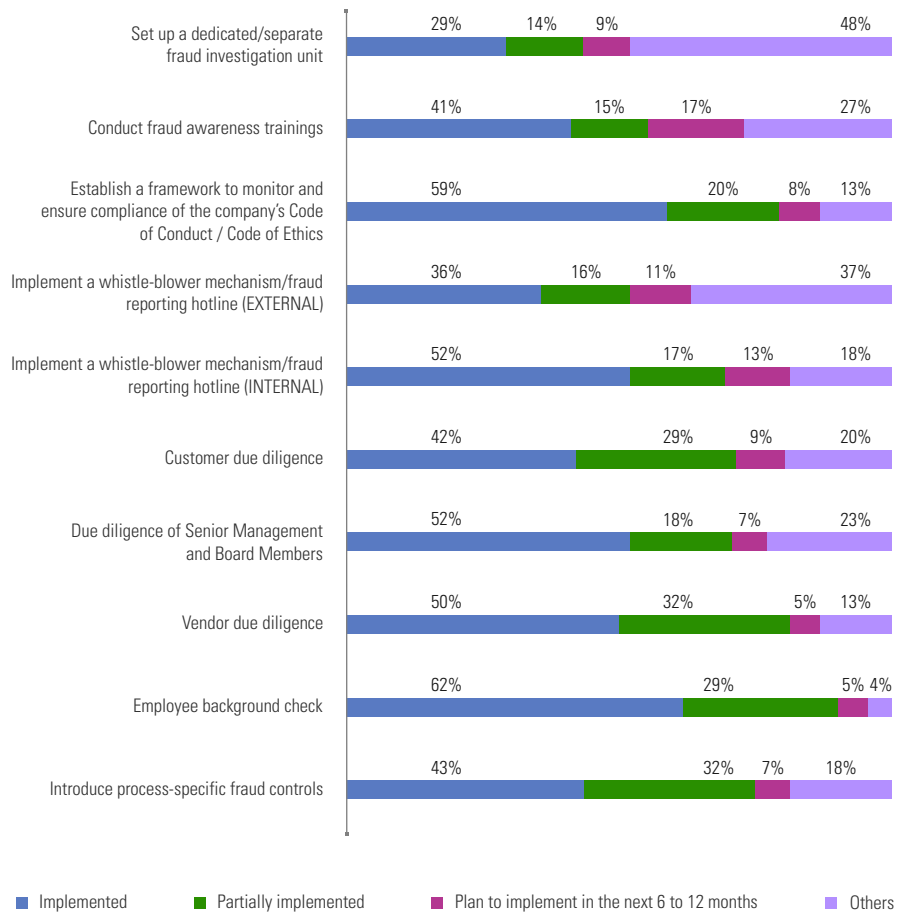
Over 70 percent of the respondents have implemented or plan to implement critical fraud prevention controls such as process specific fraud controls, employee background checks, vendor/ customer/ senior management due diligence and establishing internal whistle-blower mechanism.

70%

of the respondents have implemented or plan to implement critical fraud prevention controls

It is pertinent to note that over 50 percent of the respondents have implemented / are planning to implement additional controls like external whistle-blower mechanism and setting up dedicated fraud investigation unit.

Figure 14: Status of implementation of various control measures by respondents (multiple choice)



Others include: "Not important hence not implemented" and "Important but delayed by practical difficulties"

Source: KPMG in India's Fraud Survey 2010

Code of conduct compliance

In operationalising the code of business ethics, organisations are challenged largely due to the following:

- The organisation's reward system is mis-aligned to its core values. When it comes to performance evaluation, achievement of 'hard targets' gains precedence over ethical conduct.
- As companies pursue newer markets to take advantage of growth opportunities, cultural gaps and differences in business practices emerge which become difficult to overcome.
- The culture does not allow the discussion of difficult, controversial or sensitive matters with the senior management and the board.
- Information received by the board on whistle-blowing incidents is censored by the management and perhaps far away from the truth.

In our experience of working with organisations, there are two broad focus areas:

Communicating the code of conduct – Organisations need to continually communicate the code of conduct through a variety of means encompassing training on the code of ethics within employee induction programs, ethical dilemma workshops and annual self compliance mechanisms.

Monitoring compliance with the code of conduct – There is a perception amongst many that the code of conduct is a soft issue and incapable of being audited. Leading organisations with diversified operations are however prepared to challenge this line of thought by undertaking ethical audits. The ethical audits typically focus on:

- Areas where staff is not getting enough training on the meaning of the code.
- Areas where senior / executive management is turning a blind eye to suspected/ actual ethical breaches because of performance / results pressures, i.e. super-performers, are tolerated.
- Reflect on whether senior executives and business managers value the work of internal auditing.
- Survey if evidence on staff attitudes about the importance of control and compliance flags a disconnect between what the leadership is saying and what is actually happening.
- Monitor whether there are any trends in the issues employees are raising.

Proactive data analytics

Compared to the 2008 Fraud survey in which only 27 percent of the respondent organisations had adopted proactive data analytics for analysing e-data, this year’s survey indicates:

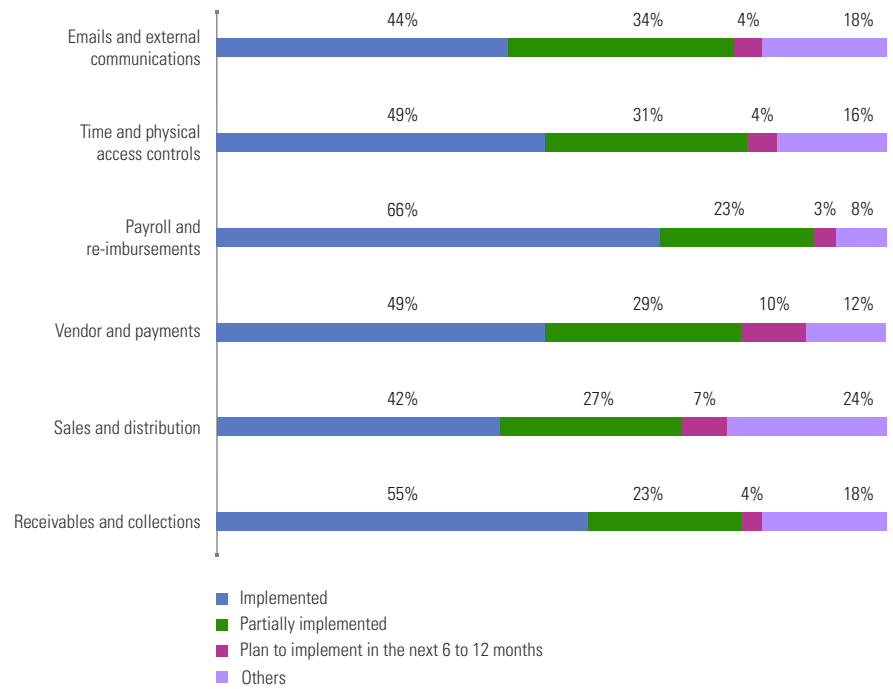
- Over 42 percent have implemented proactive data analytics in various streams in the organisation
- Over 22 percent have partially implemented data analytics in various streams in the organisation

“Technology is the best bet to drive-in transparency”

Vice President Finance of a leading Healthcare Organisation

Over 42% of respondent organisations have implemented proactive data analytics in various streams in the organisation

Figure 15: Status of implementation of proactive data analytics (multiple choice)

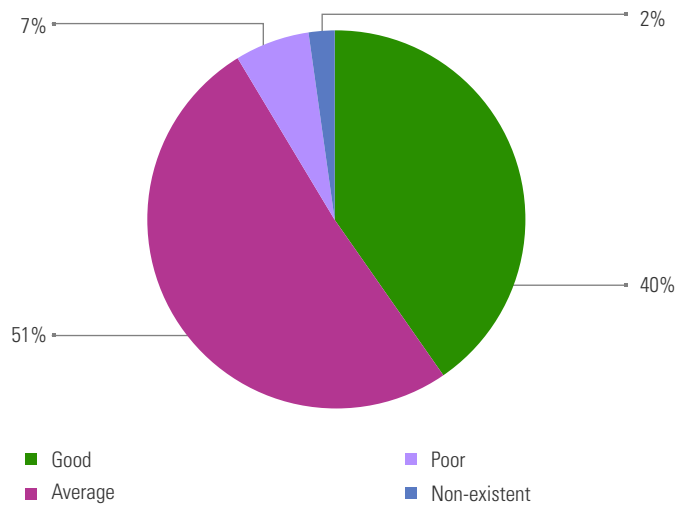


Others include: "Not important hence not implemented" and "Important but delayed by practical difficulties"

Source: KPMG in India’s Fraud Survey 2010

Leveraging technology can help strengthen corporate governance, facilitate the implementation of more effective and focused internal controls, reduce potential future losses, and help identify recoverable actual losses. 60 percent respondents believe that the current technology tools in detection of anomalies and identification of red flags or early warning signals are average to poor.

Figure 16: Current technology tools in detection of anomalies



Source: KPMG in India’s Fraud Survey 2010

Proactive data analytics

Technology has created new ways for organisations to respond to the challenge of preventing and detecting fraud and misconduct. Increasingly, companies are employing analytical techniques in their efforts. Most companies, today, prefer to be 'proactive' in leveraging data analytics. This enables them to highlight any 'red flags' and/or potential fraud before the damage is done to the organisation. Proactively analysing data also helps companies in identifying control weaknesses and fixing them upfront before these weaknesses open the possibility of a fraud or misconduct.

However, organisations considering implementing data analytics to prevent and detect fraud have to overcome the following key challenges:

- Lack of skilled resources: 'Skilled Resources' does not just mean well-trained tool-experts. Skills in understanding various analytical techniques that are available and applying them for detecting fraud requires a combination of business understanding, data understanding and adequate training on use of analytical software. Organisations have to look at building skills in all the areas to get maximum mileage from software/hardware investments made on Analytics
- Limited resources: Limited resources spread across various functions/activities limits the effectiveness of data analyses in Fraud Detection. Fraud detection should be driven with disciplined data analytics processes to address this challenge.
- Ability to evaluate the full transaction: Sampling data for fraud detection or suspicious activity detection is a wrong-start. However, the challenge to evaluate full transactions is the 'volume' of data and horse-power it requires to crunch millions of transactions businesses generate each year.
- Different systems and different data formats: Growing number and diversity of applications churn data in different formats. This data needs to be integrated in a meaningful way for proper analysis. Data integration takes a lot of time. A robust plan and

allocation of adequate resources to get the data into format ready for analysis is important.

- Definition of an anomaly: Fraud, by nature, is constantly evolving and hence there is a need to constantly update 'known' fraud scenarios, expertly monitor data analysis scenarios and then align them to business operations.
- False positives: False-positives are a serious issue in any fraud detection system. As false positives consume a lot of time and resources in resolving them, proactive data analysis has to be done to constantly suppress false positives.

Proactive data analytics involves taking routinely collected unrelated data sets and then conducting comparisons, summaries, and aggregations to detect anomalies known to be indicative of potential fraud and misconduct. Key benefits of data analytics among others include:

- Identification of hidden relationships between people, organisations, and events
- A means to analyse suspicious transactions
- An ability to assess the effectiveness of internal controls intended to prevent or detect fraudulent activities
- The potential to continually monitor fraud threats and vulnerabilities
- Analyse thousands of transactions in less time, more efficiently and cost effectively.





Shades of things to come

Survey respondents identify the following types of frauds as posing a higher risk in the coming years:

- Bribery and corruption (including kickbacks) (47 percent)
- Intellectual Property fraud (counterfeiting, piracy) (34 percent)
- E-commerce and computer related fraud (53 percent)
- Supply chain fraud (procurement and sales and distribution) (50 percent)

Bribery and corruption

Corruption is a serious offence, often not appropriately recognised by many organisations. The World Bank has estimated that, globally, bribes paid each year amount to over USD 1 trillion. Bribery and Corruption is on the risk radar of Governments, regulators, law enforcement agencies and businesses worldwide. With the increase in public scrutiny of multinational organisations, it is pertinent for companies to adopt essential controls to mitigate the risk of corruption.

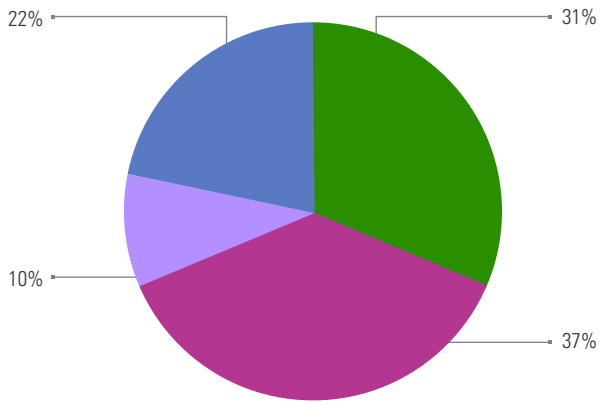
Contributing factors

Obtaining routine administrative approvals from the Government or governmental agencies and attempts to win or retain business emerge as the key reasons for bribery and corruption in corporate India.

Forty two percent of the respondents indicate that bribery has come to be considered as an acceptable behaviour. Further, 38 percent of the respondents rationalise by indicating that bribery is an

integral feature of the practices in their industry. These figures indicate the extent to which bribery and corruption has embedded itself into the way of conducting business in India. Further, over 30 percent of the respondents believe that the inadequacies in the regulatory and enforcement framework have failed to curb bribery and corruption.

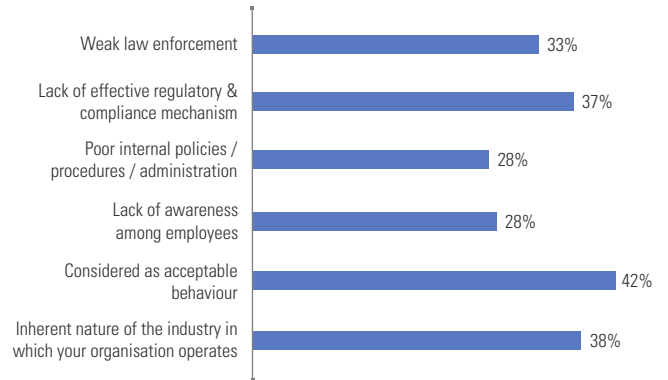
Figure 17: Common forms of bribery



- Bribery / Kickbacks to win or retain business
- Bribery to get routine administrative approvals from Government agencies
- Unauthorised use of resources
- Influence people in making/delivering a favourable treatment

Source: KPMG in India's Fraud Survey 2010

Figure 18: Factors facilitating corruption (multiple choice)



As indicated above, respondents highlight lack of effective regulatory framework, specifically weak law enforcement, as a facilitator of corruption. Companies in India are increasingly expected to adhere to Indian - Prevention of Corruption Act, 1988 and international anti-bribery laws/regulations (e.g. Foreign Corrupt Practices Act (US), Anti bribery bill (UK), owing to

their operations across the globe. Primarily these laws suggest effective policies and governance as a key measure to prevent bribery and corruption. However, compliance with these regulations is scarcely monitored.



“Corporates and industry bodies should be aggressive advocates of clean business practices. Independent bodies should rate government agencies (like international ratings of countries) against standard parameters.”

Chairman and Managing Director of a IT and Design Solution company

Knowledge of applicability of FCPA

Despite serious regulatory implications, 30 percent of the respondents were not aware if their organisation was subject to FCPA. Prevention of corruption is as much about organisational culture as it is about rules and control systems. Although there is a significant increase in awareness levels when compared to the earlier survey, it is pertinent to note that ignorance to comply with anti-corruption laws cannot protect the organisation from being prosecuted.

42%

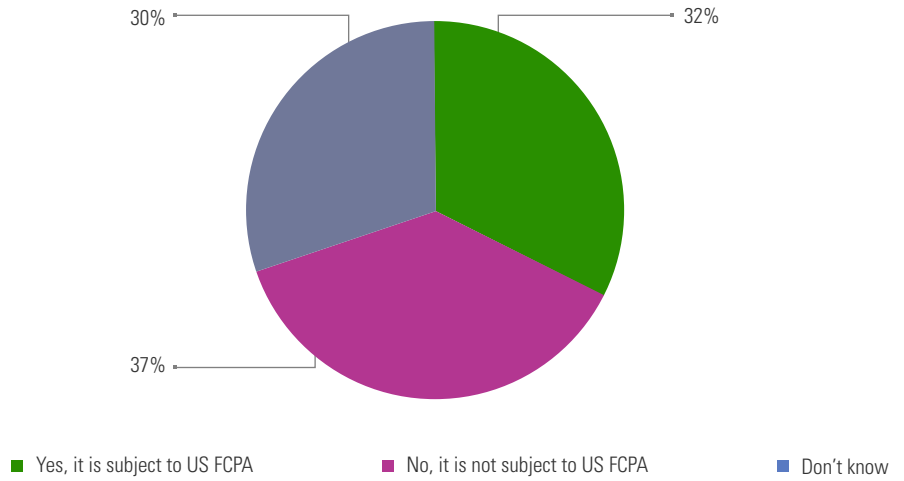
bribery has come to be considered as an acceptable behaviour

77%

India Inc. should adopt a zero tolerance approach to combat bribery and corruption, which includes legal action against perpetrators

Corruption and bribery need to be addressed at the entity level by the board and senior management. Companies should develop and promote unequivocal policies that curb bribery and encourage disclosure of facilitation payments. The way in which organisations operate with their external stakeholders (e.g. vendors, customers, regulators, tax authorities and minority shareholders) often has a tremendous bearing on how the senior management and the board are perceived internally by employees.

Figure 19: Applicability of FCPA

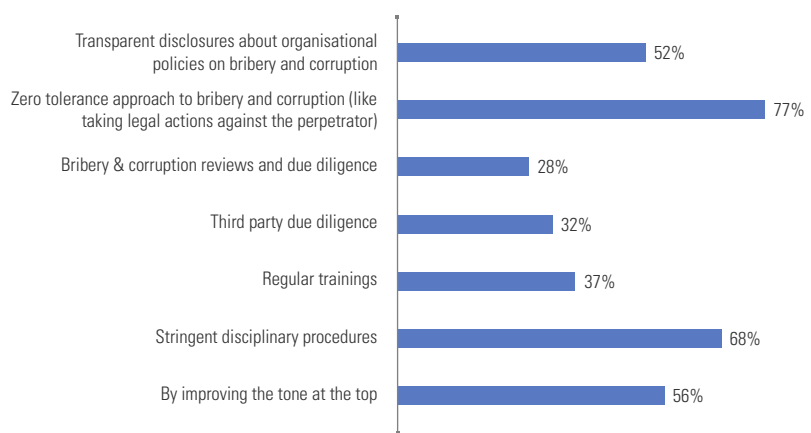


Source: KPMG in India's Fraud Survey 2010

Measures to combat corruption

Seventy seven percent survey respondents believe that India Inc. should adopt a zero tolerance approach to combat bribery and corruption, which includes legal action against perpetrators. Further, 56 percent of the respondents believe that tone at the top is crucial in establishing a corporate culture that discourages bribery.

Figure 20: Measures to fight corruption in India (multiple choice)



Source: KPMG in India's Fraud Survey 2010

"Zero tolerance to fraud, bribery and corruption is a key factor for a company's success."

Sheila Sarkar, Global Internal Audit Head, Nokia Siemens Network

Applicability of FCPA for companies in India and risks associated with facilitation payments

Applicability of FCPA to companies in India

Broadly, FCPA is applicable to:

- Companies listed in U.S including foreign companies or foreign affiliates that are listed on US stock exchanges ('Issuer').
- Subsidiaries and joint ventures in which the issuer has significant share.
- Agents, business partners, contractors of the issuer or foreign affiliate or subsidiaries/ joint ventures of the issuer.

FCPA is becoming increasingly applicable to many companies in India. As more and more Indian companies expand into foreign markets, it becomes imperative for these companies to gain a good understanding of the regulatory environment in these markets, specifically regulations around bribery and corruption.

FCPA primarily prohibits payment of bribes to foreign officials (Government officials including representatives of Government or Government owned entities). The lack of awareness of foreign bribery and corruption regulations has been identified as a major reason in some recent bribery and corruption related prosecutions.

Bribery and facilitation payments are interrelated as these refer to any payments made for influencing a person to act favourably.

Facilitation payments

Facilitation payment is a form of pay offs made to a public official to expedite or facilitate routine governmental actions/ approvals. Facilitation payments are

normally not intended to obtain or retain business. These payments are normally demanded by junior public officials.

While FCPA does not prohibit facilitation payments, Prevention of Corruption Act, 1988 ('PCA' - Indian Anti-Corruption Law), prohibits such payments. However, in practice the PCA has not been strictly enforced with respect to such payments. Therefore facilitation payments have been considered an acceptable way of conducting business in India. In the past, businesses would have rather paid bribes than face bureaucratic delays.

However, the challenge which companies have is being compliant while remaining competitive in the marketplace. Companies can meet these challenges by establishing policies and training programs to ensure compliance with anti bribery and corruption laws. Such programs must include:

- a commitment from the "top down" that bribery in any form will not be tolerated
- designation of a Compliance Officer to address questions and oversee reviews and audits of company procedures
- targeted training for those who interact with public officials or their agents, managers and supervisors, and financial analysts
- proper evaluation of vendors and agents, to ensure compliance with anti-bribery law
- background checks of business partners to ensure legitimacy

Although these steps are not exhaustive, they serve as a reminder that compliance can be achieved once a commitment is made to abide by anti-bribery laws.

Intellectual Property fraud

In today's knowledge intensive economy where innovation and technology are viewed as key differentiators, it is not surprising to witness a dramatic increase in intangible assets, especially Intellectual Property, as a proportion of the total assets. As the significance of Intellectual Property increases, the accompanying risks, especially fraud risk, also dramatically increase.

Maximum number of respondents identified counterfeiting and parallel supply chain as the most prevalent form of IP fraud. Companies in consumer market segment and IT space suffer severely on this account and lose a large amount of revenue on this account every year.

43%

Identify ambiguous nature of IP laws as a major factor that facilitates IP fraud

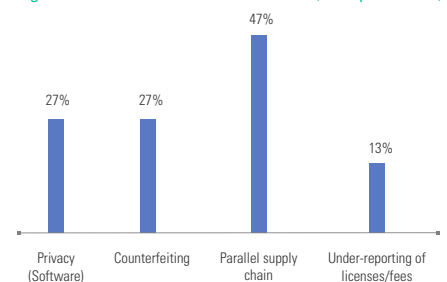
Contributing factors

While respondents identify IP fraud as an emerging area of concern, 43 percent of the respondents identify ambiguous nature of IP laws as a major factor that facilitates IP fraud. Additionally, 62 percent of the respondents identify weak enforcement of IP laws as another key stumbling block.

39%

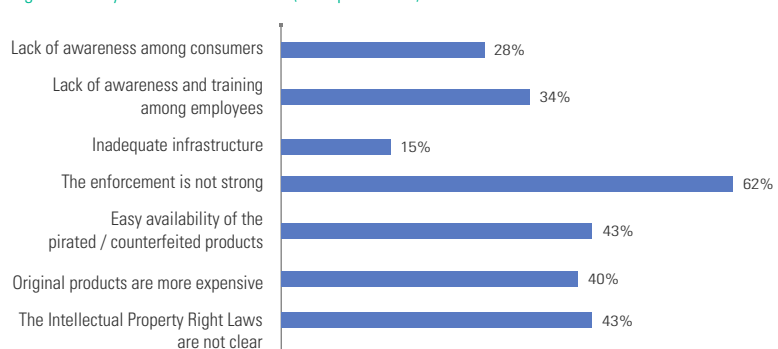
Identify competitors as a key perpetrator of IP frauds

Figure 21: Common forms of IP frauds (multiple choice)



Source: KPMG in India's Fraud Survey 2010

Figure 22: Key reasons for IP frauds (multiple choice)

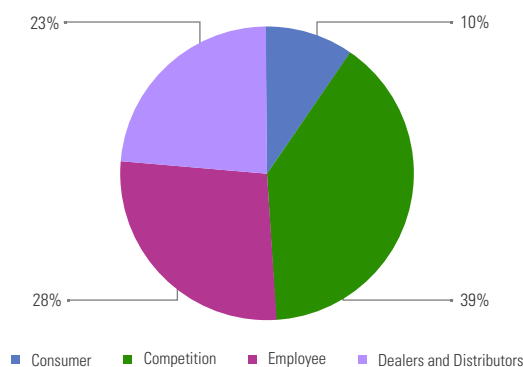


Source: KPMG in India's Fraud Survey 2010

Key perpetrators

While 39 percent of the respondents identify competitors as a key perpetrator of IP fraud, 28 percent identify employee as a key perpetrator.

Figure 23: Major threat of IP fraud



Source: KPMG in India's Fraud Survey 2010

Counterfeiting and parallel supply chain

Illegal replicas of branded products are flooding the market place, cutting into companies' revenues and hampering their ability to invest in research and development.

How counterfeiting affects the organisation:

- Counterfeiting is one of the most significant threats to the free market. It not only steals the value of intellectual capital, it also stifles innovation and robs the customer of the quality they expect from the brand.
- Worldwide, inconsistency of standard practices relating to Intellectual Property rights creates significant challenges for businesses wishing to protect their innovations, brands, and processes in global economy.
- The increasing threat of counterfeiting has a direct impact on the brand equity, and the reputation of an organisation. By reducing revenue and damaging brand equity, counterfeiters of branded products are eroding the integrity of supply and demand business model.

Among other risks, counterfeiting in supply chain has significant impact on the brand reputation of the product in question. The companies should organise:

- In depth field investigations on brand protection aiding in understanding and mapping the illegal supply chain, identifying key players that operate within the supply chain, and taking corrective action against perpetrators on the basis of accurate and in depth intelligence collected from the market.
- Conducting surprise field visits to assess the availability of counterfeit products.
- Channel reviews of the supply chain to help ensure there are no apparent leakages from the supply chain and no apparent involvement of channel partners in counterfeiting.
- Effective strategy needs to be broad based which should aim to attack the counterfeit operations from as many angles as possible.



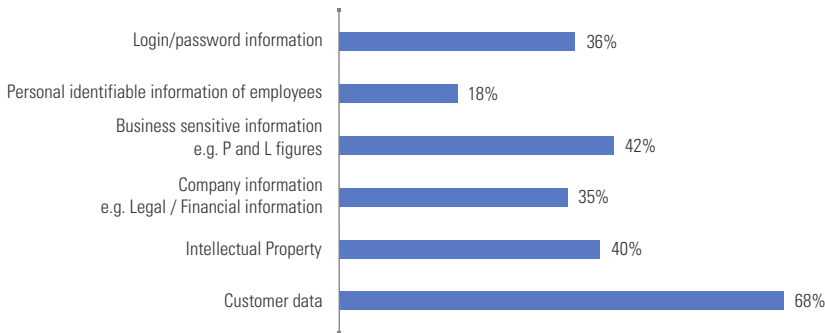
E-crime

While, on one hand, technology tools assist companies in enhancing productivity and efficiency, on the other it increases their vulnerability to sophisticated cyber crime attacks. Electronic crimes weaken the organisation's IT backbone. For instance, theft of customer information from a company's computer system could not only expose the company to litigation risks but also to reputation risks that could cripple the company's business.

While 68 percent of the respondents believe that customer data could be classified as an asset with a high risk of an electronic attack, 42 percent believe business sensitive information such as profit and loss figures could be classified as a high-risk target.

Further, 52 percent of the respondents indicate emails as a component of the IT infrastructure that has the highest vulnerability in terms of potential exploitation by cyber criminals. Additionally, while 43 percent identify internet as another vulnerable component of the IT infrastructure, 36 percent identify applications hosted on the web as a vulnerable component.

Figure 24: Key business assets that are targets of electronic attacks (multiple choice)

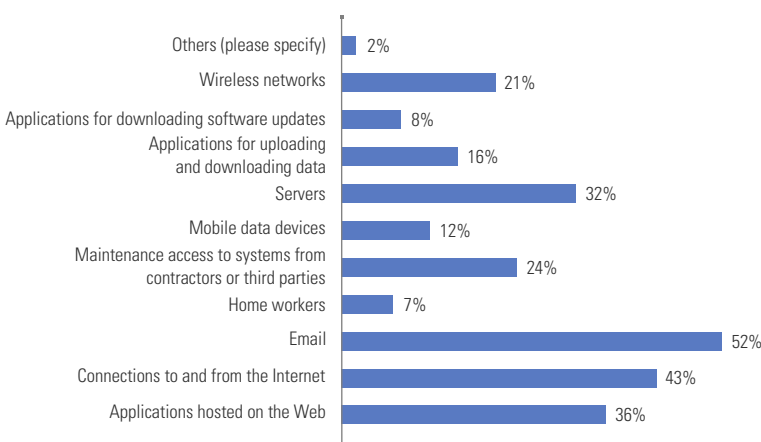


Source: KPMG in India's Fraud Survey 2010

68%

Believe that customer data could be classified as an asset with a high risk of an electronic attack

Figure 25: Components of IT infrastructure and their vulnerability to e-crime (multiple choice)



Source: KPMG in India's Fraud Survey 2010

52%

Emails are highly vulnerable in terms of potential exploitation by cyber criminals.

Supply chain fraud

Today's globalised and intertwined markets have vastly contributed to increased business complexities, especially in the area of supply chain. The risk of supply chain extends from primary sourcing of the raw material to the distribution of the finished products. In fact, survey respondents, as discussed previously, have rated supply chain (procurement and sales and distribution) as the most vulnerable areas for fraud.

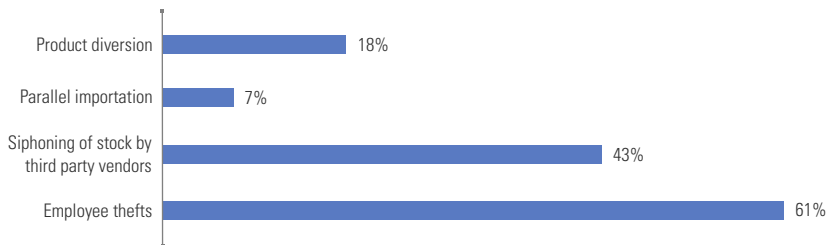
Forms of supply chain fraud

Among the various forms of supply chain frauds, employee theft is viewed as most common, with 61 percent of the respondents experiencing this form of fraud. Additionally, 43 percent indicate that fraudulent activities in the supply chain were committed by third parties by siphoning off stocks, through stock pilferage.

Contributing factors

While 66 percent of the respondents identify lack of effective internal controls as the main reason for supply chain leakage/fraud, 36 percent of the respondents indicate lack of appropriate inventory management system as a reason. Additionally, 34 percent of the respondents identify lack of due diligence on third parties as one of the key reasons for the fraud.

Figure 26: Forms of supply chain fraud (multiple choice)



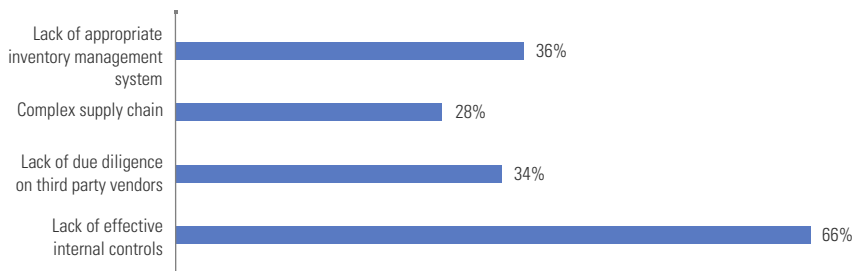
Source: KPMG in India's Fraud Survey 2010

61%

Employee theft is the most common form of supply chain fraud



Figure 27: Key reasons for leakage in supply chain (multiple choice)



Source: KPMG in India's Fraud Survey 2010

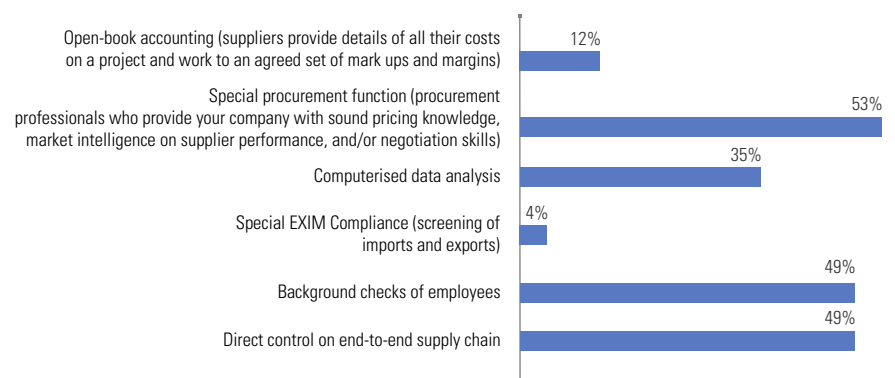
While entering into a sourcing relationship, a company must ensure that a comprehensive due diligence is conducted on the supplier and that they are adhering to the company's code of conduct. Moreover, while it is important to know the business partner prior to developing a relationship and signing a written contract, it is also essential to regularly monitor third party activities by conducting regular audits and performance evaluations.

Fifty three percent of the respondents indicated that establishing a special procurement function with specialists as a key preventive measure to mitigate supply chain fraud risk. Direct control on end-to-end supply chain (49 percent) and initiating background checks of employees/ suppliers (49 percent) can aid in mitigating the supply chain fraud risk.

49%

Conducting background checks of employees and suppliers can aid in mitigating the supply chain fraud risk.

Figure 28: Preventive measures to reduce fraud in supply chain (multiple choice)



Source: KPMG in India's Fraud Survey 2010

Enhancing integrity in supply chain

As indicated by the respondents supply chain is one of the riskier functions of the organisation. Supply chain disruptions directly impact the revenue, market share and costs associated with distribution.

With growing business needs and footprints in various markets the supply chains are becoming more complex thereby enhancing the risk of fraud at various touch points. Fraud risks in supply chain can occur during the procurement (or sourcing) of the products, inventory or storage or during the sales and distribution.

Procurement

Historically companies have seen procurement as merely a transactional arm to place purchasing orders and to manage contracts instead of a function really to drive profitability. However, this needs to be changed as companies need to view this as an integral part of the supply chain. Depending on the nature of your business, you may be susceptible to certain risks such as

- phantom vendors: where fictitious vendors are set up in your vendor master file and a list of payments are made.
- bid rigging: where there's collusion between your procurement personnel and the bidders.
- grey market: where counterfeits and knockoffs can occur or where your suppliers generate unauthorised production putting your products at risk.

Sales and distribution

Theft of goods is a common phenomenon in supply chain industry. With stocks spread at multiple locations and in transit, companies face difficulty in preventing stock losses or thefts. Further the employees in connivance with the distributor get involved in theft of goods

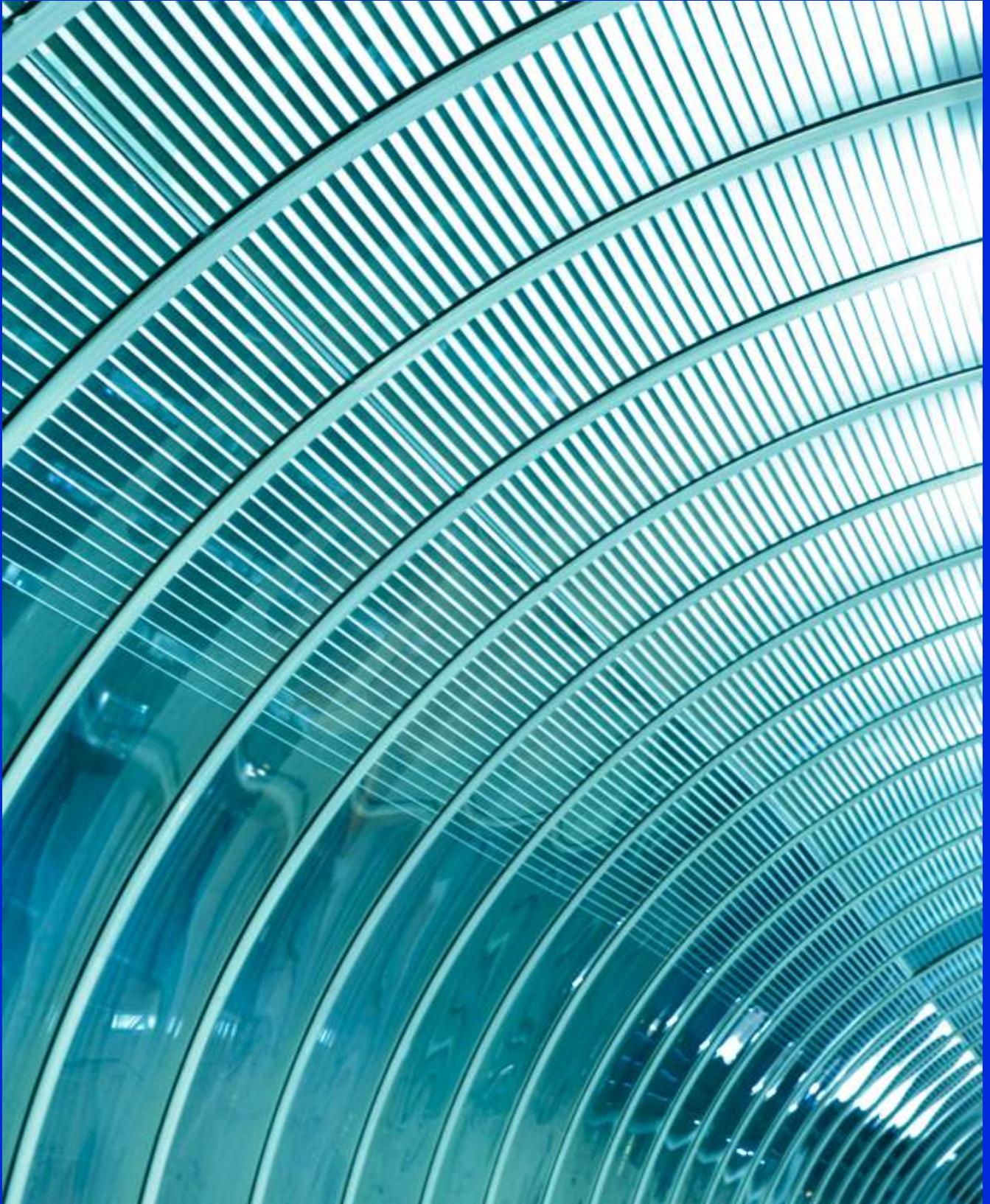
or distribution of stock at prices less than fixed by the company. Disproportionate cost of distribution to that of the market share and undisclosed conflict of interest with distributors are key indicators of these types of frauds.

Another challenge faced by the companies today is on the channel management as most of these relationships are self reporting. Based on KPMG's experience 70 percent of the self reported statements are incorrect.

What are the red flags of supply chain fraud

Some indicators could be as follows:

- Reluctance to change the vendor/distributor by employees
- Low quality of goods procured at high prices
- Unusual increase in sales towards end of the financial year
- Different prices in the market than prevailing price of the company
- Poor documentation pertaining to stock handling
- Frequent complaints or return of goods
- Quantity sold by retailers in the market are more than the maximum stock sold to wholesale distributor at any point in time
- Sales/ procurement staff demanding more lead time before getting prepared for an audit



Conclusion

In summary, the fallout from fraud and misconduct can be significant, including punitive damages, tarnished corporate and brand image, lost revenue, plummeting shareholder value and inability to attract and retain human capital.

To combat frauds effectively, organisations need to adopt a holistic approach that takes cognizance of fraud risks emanating from the organisation's strategy and the adequacy of mitigating measures at multiple levels i.e. entity level, process level and functional level controls.

Despite the apparent awareness of the risks posed by a multitude of fraud types as indicated by this survey, organisations tend to focus more on the adequacy of controls mitigating financial frauds and there is a considerably lesser focus on anti-fraud programs and controls to mitigate non-financial fraud risks.

Adequacy of controls

Industry Segments	Types of Frauds				
	Financial Statement Fraud*	Bribery and Corruption*	IP Fraud*	E-Crime*	Supply Chain Fraud*
Consumer Markets					
Information, Communication & Entertainment					
Real Estate & Infrastructure					
Financial Services					
Industrial Markets					

*Degree of adequacy depicted by "Harvey Balls" based on score: 95-100: 1; 75-94: ¾; 50-74: ½; 25-49: ¼; < 25: 0. Score indicates the percentage of survey respondents who rated their control measures for the aforementioned fraud types as "adequate".

50%

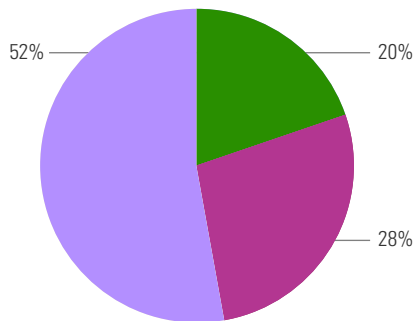
Controls for managing IP fraud, supply chain fraud, e-crime and bribery and corruption risks needs improvement or are non-existent

At the organisational level (senior management and the Board), it is important to have a comprehensive approach to fraud risk management which also considers the organisation's preparedness in terms of skills, tools and technology to implement the desired control mechanisms. In other words, implementation and intent need to go hand in hand to combat fraud effectively.



Profile of respondents

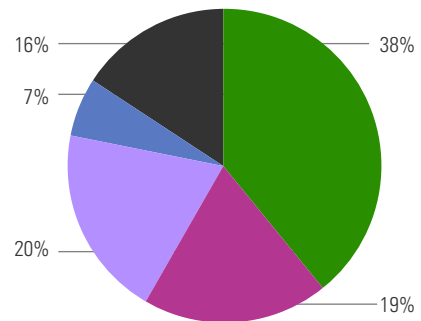
Profile of respondent organisation



■ An Indian firm with only domestic operations
 ■ An Indian Multinational
 ■ Multinational

Source: KPMG in India's Fraud Survey 2010

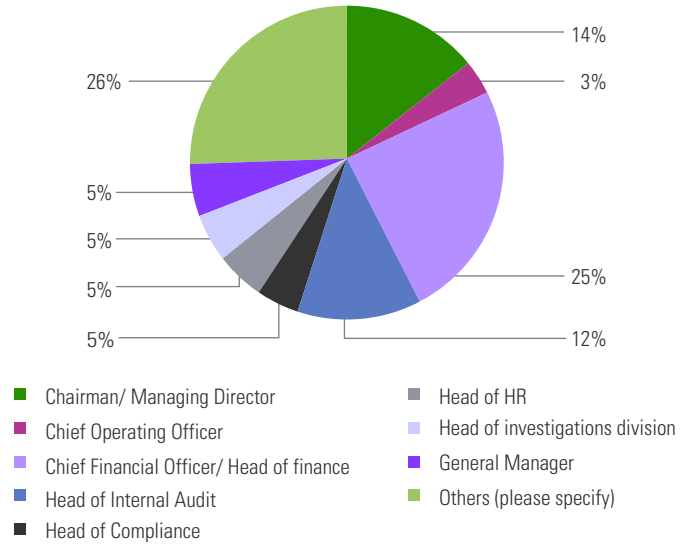
Annual turnover of respondent organisations



■ < INR 500 crore
 ■ INR 500 crore - INR 1000 crore
■ INR 1000 crore - INR 5,000 crore
 ■ INR 5,000 crore - INR 10,000 crore
■ > INR 10,000 crore

Source: KPMG in India's Fraud Survey 2010

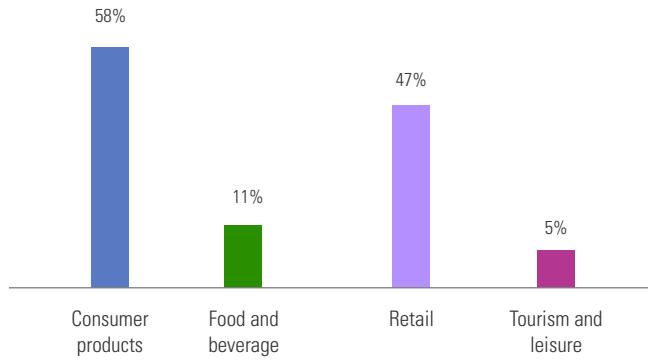
Profile of respondents



Source: KPMG in India's Fraud Survey 2010

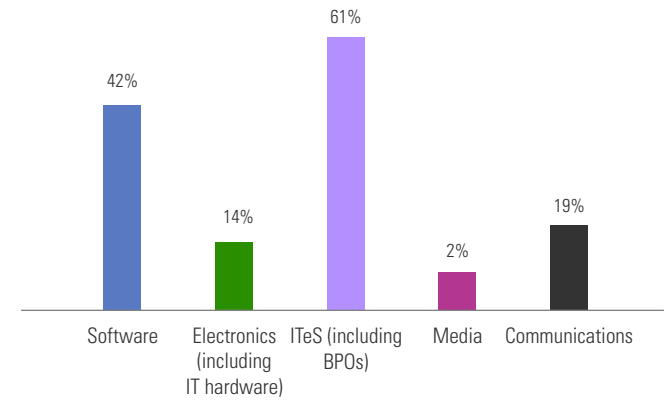
Industries that respondents represent (multiple choice)

Consumer Markets



Source: KPMG in India's Fraud Survey 2010

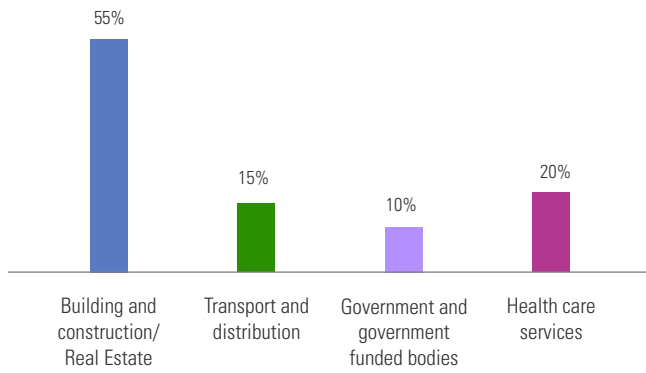
Information, Communication & Entertainment



Source: KPMG in India's Fraud Survey 2010

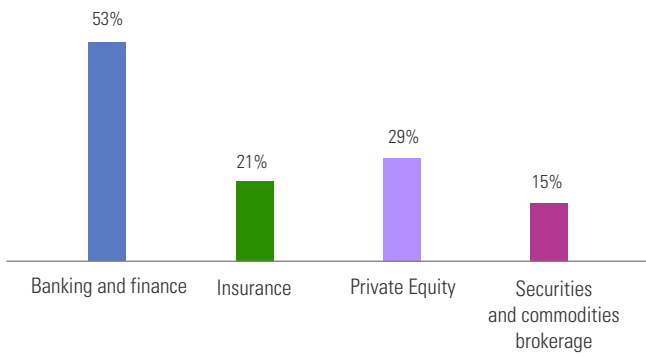
Industries that respondents represent (multiple choice)

Real Estate and Infrastructure



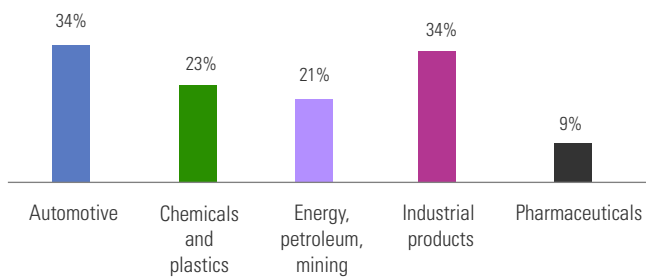
Source: KPMG in India's Fraud Survey 2010

Financial Services



Source: KPMG in India's Fraud Survey 2010

Industrial Markets



Source: KPMG in India's Fraud Survey 2010





KPMG in India

Mumbai

Lodha Excelus,
Apollo Mills Compound,
N.M. Joshi Marg, Mahalaxmi
Mumbai 400 011
Tel: +91 22 3989 6000
Fax: +91 22 3983 6000

Delhi

Building No. 10, 8th Floor
Tower B, DLF Cyber City
Phase II, Gurgaon
Haryana 122 002
Tel: +91 0124 307 4000
Fax: +91 0124 3074300

Pune

703, Godrej Castlemaine
Bund Garden
Pune - 411 001
Tel: +91 20 3058 5764/65
Fax: +91 20 3058 5775

Bangalore

Maruthi Info-Tech Centre
11-12/1, Inner Ring Road
Koramangala, Bangalore – 560 071
Tel: +91 80 3980 6000
Fax: +91 80 3980 6999

Chennai

No.10, Mahatma Gandhi Road
Nungambakkam
Chennai - 600034
Tel: +91 44 3914 5000
Fax: +91 44 3914 5999

Hyderabad

8-2-618/2
Reliance Humsafar, 4th Floor
Road No.11, Banjara Hills
Hyderabad - 500 034
Tel: +91 40 3046 5000
Fax: +91 40 3046 5299

Kolkata

Infinity Benchmark, Plot No. G-1
10th Floor, Block – EP & GP, Sector V
Salt Lake City, Kolkata 700 091
Tel: +91 33 44034000
Fax: +91 33 44034199

Kochi

4/F, Palal Towers
M. G. Road, Ravipuram
Kochi 682 016
Tel: +91 484 302 7000
Fax: +91 484 302 7001

KPMG Contacts

Richard Rekhy

Head of Advisory
Tel: +91 124 307 4303
e-Mail: rrekhy@kpmg.com

Vikram Utamsingh

Head of Markets
Tel: +91 22 3090 2320
e-Mail: vutamsingh@kpmg.com

Deepankar Sanwalka

Head of Risk & Compliance Group
Tel: +91 124 307 4302
e-Mail: dsanwalka@kpmg.com

Rohit Mahajan

Executive Director, Forensic Services
Tel: +91 80 3065 4200
e-Mail: rohitmahajan@kpmg.com

Dinesh Anand

Executive Director, Forensic Services
Tel: +91 124 307 4704
e-Mail: dineshanand@kpmg.com

Vivek Subramanian

Executive Director, Forensic Services
Tel: +91 22 3090 2390
e-Mail: viveksubramanian@kpmg.com

Gaganpreet Puri

Executive Director, Forensic Services
Tel: +91 124 307 5011
e-Mail: gpuri@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2010 KPMG, an Indian Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

KPMG and the KPMG logo are registered trademarks of KPMG International Cooperative ("KPMG International"), a Swiss entity.

Printed in India