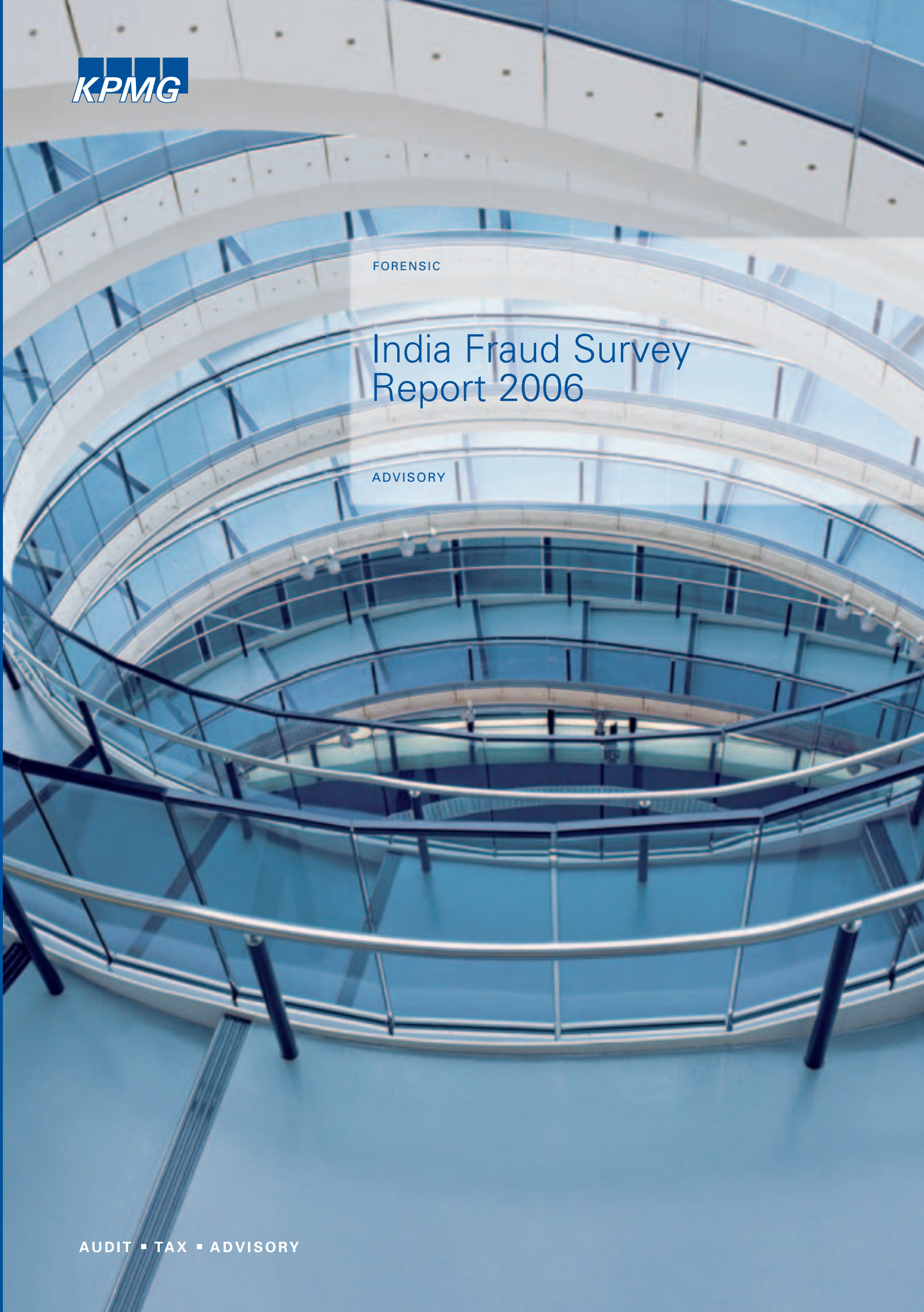


KPMG

FORENSIC

India Fraud Survey Report 2006

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

KPMG Forensic, India

KPMG's Forensic practice in India was established in 1995. The practice has over time evolved into a team of over 35 dedicated forensic professionals, each one bringing in not only a rich and extensive experience but also a competitive and specific skill set. We have professionals which include certified fraud examiners, former police officers, chartered accountants, CPAs, MBAs, business ethics professionals, social workers, technology professionals and lawyers. Our team members have working experience on engagements both at national and international levels in the US, Canada, UK, Singapore, Europe, Middle East, Mauritius and South Asian countries.

The team brings in over 150 man years of collective investigative experience on the basis of which they have provided practical and prudent advice on various assignments across industry sectors and different lines of businesses.

KPMG's Forensic practice endeavours to provide an independent, proactive and responsive service, together with credible results by effectively utilising its investigative, IT, accounting, financial and various other resources towards the detection and investigation of alleged fraud and in resolving commercial and legal disputes. We emphasise on a need for innovation, flexibility and quality along with providing credible evidence to help companies make informed decisions.

The services provided by us include:

- Fraud investigations
- Fraud and misconduct diagnostic reviews
- Forensic technology services
- Corporate intelligence
- Pre employment background check
- Dispute resolution, litigation support and expert witness services
- Anti - money laundering compliance
- Business ethics services
- Contract compliance services
- Supply chain integrity
- Asset tracing

For further information please contact:

Deepankar Sanwalka
Executive Director
KPMG
4B, DLF Corporate Park
DLF City, Phase III
Gurgaon 122 002
Telephone : +91 124 254 9191
Fax : +91 124 254 9195

Preface

KPMG's Forensic practice in India has been undertaking country focussed studies and surveys to assess the overall level of awareness of fraud and the means to mitigate the fraud risks amongst senior management in corporate India.

As one of the leading provider of forensic services, KPMG believes that it is important to quantify the trend, nature and extent of fraud in today's business environment. Our experience in the recent past clearly demonstrates that there is a reduced tolerance to fraud and non ethical behaviour as well as a clear shift from reactionary measures in combating fraud to proactive measures in mitigating the fraud risk. Corporate India has also shown a greater willingness to confront and tackle issues of fraud, misconduct and unethical behaviour rather than sweeping them under the carpet.

Organisations today face a completely different set of challenges — globalisation, rapidly evolving technology, rapid development in industry and business, risks and complexity of information and data management; the list is endless. With this changed scenario, the risks faced by organisation increase many fold and there arises the need to manage and mitigate this risk more effectively.

Our survey has attempted to capture the impact on corporate India due to the changed regulatory environment brought about by initiatives like Clause 49 (by the SEBI) and the Sarbanes Oxley Act (in the USA), as well as the higher levels of expectations for transparency, ethics and proactive fraud management.

We hope that you find the results of this survey as insightful as we have had. For those who would use these results, we would like to thank you for your interest in our survey concerning one of today's major business issues; also 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 those who took part in the survey.

Ian Gomes
Country Managing Director
KPMG India

Table of contents

Executive summary

The KPMG Forensic Survey 2006 is an attempt to provide a definitive insight on the antecedents of fraud, its aftermath and most importantly the measures to safeguard against fraud. The findings set out in this report were derived by means of responses to a questionnaire sent in January this year to India's largest organisations across public and private sectors. The questionnaire sought information ranging from the impact of changed regulatory environment to levels of expectations for transparency and ethics to the fraud incidents in the respondent's organisations during the previous year.

A summary of our key findings is given below:

- The responses brought out that fraud risk was perceived to be highest for the financial sector (banking, insurance, mutual funds, asset management companies, NBFCs and investment banks) followed by the information communication and entertainment sector (telecom, media and software). On the other hand sectors like transportation, retail, consumer and food were amongst the lower fraud risk areas.
- It was observed that the maximum threat of fraud was perceived from the employees, as has been brought out from previous studies.
- Lack of ethical values was cited as one of the principal reasons for the occurrence of fraud in organisations. This clearly indicates the need for organisations and its employees to proactively move towards the creation of a more "ethical workplace".
- The survey showed that a majority of the respondents agreed that SOX/ Clause 49 had a marked impact on their outlook towards the risk of fraud which has urged them to undertake measures to reassess the effectiveness of internal controls and mitigate fraud risks. The responsibility of ensuring compliance with these regulations generally lies with the Board of Directors. However, it was surprising to note that a majority of the respondents had not been imparted any form of training or awareness programme which would have assisted them during the implementation of the SOX/ Clause 49 requirements.
- While most of the respondents considered their control mechanisms for protection of IP to be average almost one in every five felt that there is a scope for improvement.
- The survey also established that organisations now have begun to acknowledge the importance of conducting background checks for employees who have access to sensitive information or restricted areas.
- Survey results showed that cases of concealment of correct information by the potential applicants are still considerably high and a large proportion of organisations were not able to uncover such misleading information.
- Most of the respondents did not have any formal fraud response plan in place to minimise the impact of fraud.

- A majority of the respondents considered their IT access controls to be fairly effective. Almost 60 percent of the respondents had allocated less than 25 percent of their annual security budget to IT security.
- The survey results indicate that a significant number of frauds were either detected by the internal audit department or were reported by third parties. This perhaps suggests that an organisation's fraud control programme should allow external parties to report allegations or suspicions of fraud.

The survey findings are conclusive in establishing that fighting fraud and mitigating fraud risk is gaining importance for organisations across sectors and industry since organisations are waking up to the fact that the very existence of fraud in any form may threaten their viability and also have a bearing on their profitability. Corporate India, now, wants to act proactively and understand and execute the various measures which could help them safeguard against the perils of fraud and misconduct.

About the survey

In January 2006, KPMG's Forensic practice sent a fraud survey questionnaire to over 1,000 organisations across India which included some of the largest private sector companies, public sector companies and other organisations. The survey was conducted on a confidential basis on the undertaking that no information would be released on individual survey responses (information pertaining to the respondent or the company were not sought).

The survey aimed at:

- determining trends;
- analysing the impact of recent events like emergence of Sarbanes Oxley Act (SOX) or Clause 49 (by SEBI);
- establishing whether fraudulent activities are increasing or decreasing;
- understanding the extent and financial impact of fraud;
- understanding who is most likely to commit fraud;
- understanding how the risks emanating from offshoring and cyber crime are mitigated;
- understanding how organisations are themselves tackling the problem.

For the purpose of this survey, 'fraud' is defined as:

Any dishonest activity involving the extraction of value from a business, directly or indirectly, regardless of whether the perpetrator benefits personally from his or her actions.

Participants of this survey were required to respond to questions encompassing the following key areas:

- Existing corporate environment and fraud risk
- Impact of SOX/ Clause 49 and fraud mitigation
- Fraud risks of outsourcing/ offshoring and background checks
- Cyber security
- Frauds experienced by Indian companies in the recent past
- Responsibility for fraud control

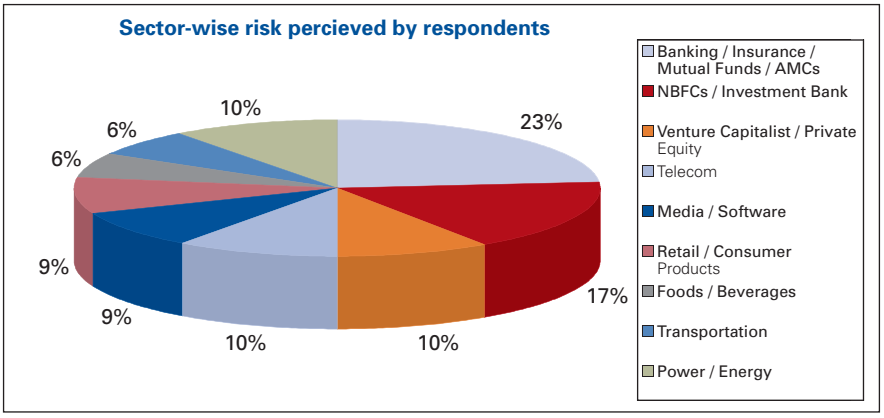
Corporate environment and the risk of fraud

The fraud risk threat is perceived to be highest in the financial sector followed by the information, communication and entertainment sector.

Sector analysis

The survey results indicated that unlike the previous survey (2002) findings where the fraud risk was perceived to be highest in the retail sector, now the fraud risk threat is perceived to be highest in the financial sector followed by the information, communication and entertainment sector.

The threat perception for these sectors is generally higher mainly on account of the nature of their business and the high growth rates achieved by these sectors in the last few years.



Within the financial sector 23 percent of the respondents believed that Banking, Insurance, Mutual Funds and Asset Management Companies (AMCs) are the most vulnerable to fraud risk while 17 percent believed that NBFCs/ Investment Banks were more vulnerable to fraud risk.

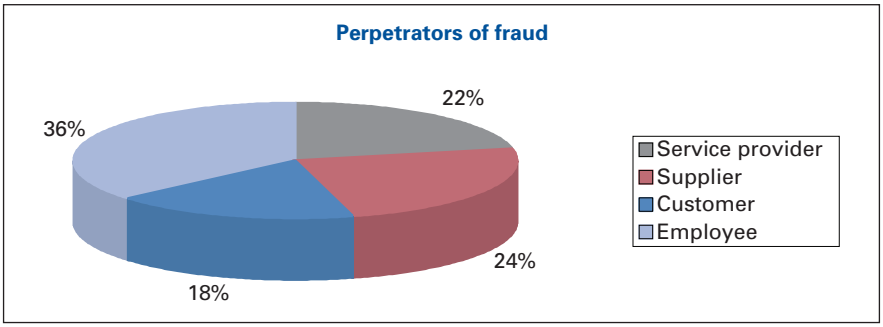
In the last 2-3 years, sectors like venture capital, private equity and telecom have had a tremendous growth. Consequently, the fraud risk threat (as perceived by the respondents) is also higher than the other sectors like retail, food and transportation.

While the respondents have indicated that sectors like transportation, retail, consumer and food are not amongst the high fraud risk areas, in our opinion this is only relative and is lower since the fraud risk perceived in the other areas is higher.

Who are the perpetrators?

We asked the respondents to identify the likely perpetrator of fraud. We provided them with options which included service providers, suppliers, customers and employees.

The respondents indicated that the maximum threat was perceived from the employees and the least from the customers.



The above results are consistent with the findings of the investigations undertaken by us in the recent past, wherein most cases it was seen that the perpetrator of the fraud was found to be either the employee in collusion with suppliers or the employee himself.

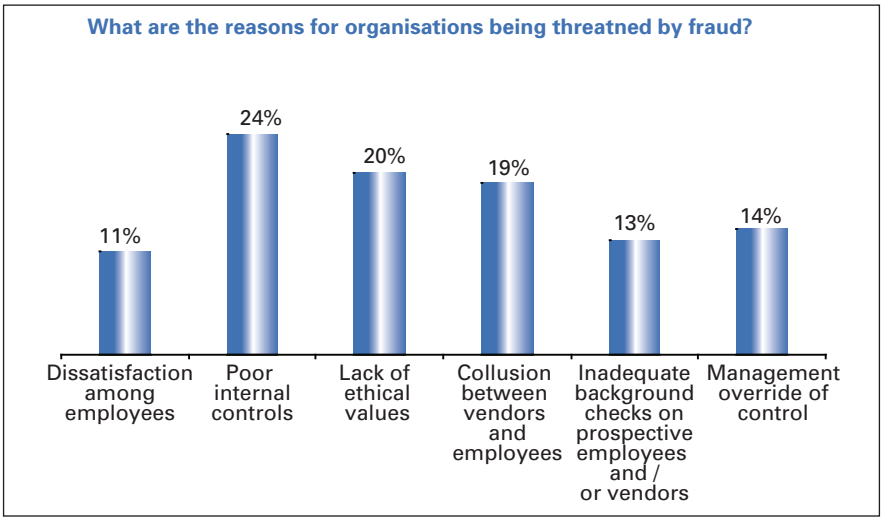
However, it was observed that to a large extent the potential threat was also dependent on the sector in which the organisation operated. For example, the maximum threat faced by:

- a BPO was from its employees;
- the financial services sector was from its customers;
- the construction sector was from its suppliers (contractors);
- the media was from employees as well as suppliers.

Why are organisations threatened by fraud?

Effective internal controls have always been considered as the first defence against fraud. In addition, ethical values among the employees to a great extent can deter the desire of financial gains through deceptive or fraudulent means.

We were interested to find out from respondents, what were the likely reasons for organisations being threatened by fraud.



Lack of ethical values has also been identified as one of the main reasons for frauds in organisations.

The respondents indicated that the weak internal controls (24 percent) and lack of ethical values among the employees (20 percent) were the major threatening factors for organisations.

The respondents clearly continue to consider that companies get defrauded mainly on account of poor internal controls. This has been consistently identified as the main reason for frauds occurring in an organisation in the previous surveys conducted by us.

Lack of ethical values has also been identified as one of the main reasons for frauds in organisations. This clearly indicates the need for organisations and its employees to proactively move towards the creation of a more "ethical workplace".

The findings of the investigations and misconduct reviews undertaken by us have also revealed that more often than not, the employees are involved in the fraud. This is a cause for concern since it implies that the very people entrusted with the responsibility of running an organisation are the perpetrators of the fraud themselves.

Fraud threatens the viability and profitability of every organisation. Organisations need to adopt a methodology to identify and address the risks of fraud. Some of the areas that a good fraud risk management process should cover are:

- A sound ethics policy and code of conduct
- A well defined whistleblowing policy
- Periodic fraud risk assessments
- A good internal audit function
- A pre-employment screening

SOX/ Clause 49 – effective tool in fraud identification/ mitigation

Organisations in India have been forced to take measures to reassess their effectiveness of internal controls and mitigate the fraud risks in view of the various provisions or requirements of SOX and/ or Clause 49.

What is Clause 49 compliance?

Clause 49 forms part of the Listing Agreement laid down by the Securities and Exchange Board of India (SEBI). It attempts to raise the standards of corporate governance of Indian companies by introducing proper risk management and internal control mechanisms. It also sets down ground rules for the structuring of the Board of Directors, Audit Committees, CEO/ CFO certification on the effectiveness of internal controls, etc. Companies have to file quarterly compliance reports and the statutory auditors need to certify this compliance.

What is SOX compliance?

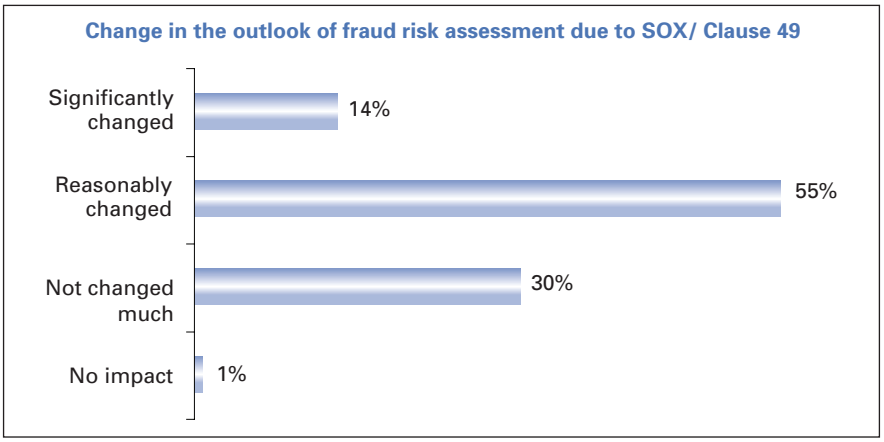
Under Section 404 of the Sarbanes Oxley Act (SOX), the management must support its evaluation of internal controls with appropriate documentation and present a written assessment as to the effectiveness of internal control over financial reporting, as at the end of the company's most recent fiscal year.

The respondents were asked questions around SOX and Clause 49 to determine the change (if any) towards their outlook of fraud risk assessment, to understand as to who was responsible for implementation in the organisation and finally whether the controls/ measures were adequate, etc.

An analysis of the responses has been provided in the following paragraphs.

Change in outlook

Organisations in India have been forced to take measures to reassess their effectiveness of internal controls and mitigate the fraud risks in view of the various provisions or requirements of SOX and/ or Clause 49. Hence it is not surprising to note that almost all the respondents agreed that SOX/ Clause 49 had some impact on their outlook towards fraud risk, as has been indicated in the graph below.



The impact was almost the same for large as well as the small organisations (organisations employing more than 1000 employees have been considered as large).

Responsibility of ensuring compliance

The role of the Board of Directors and the Audit Committees has significantly changed in the last few years. With this changed role, more and more organisations are assigning them the responsibility of implementing proactive measures to mitigate the fraud risk. Their new role requires them to implement SOX and/ or Clause 49 requirements, define code of conducts and whistleblower policies, set out fraud control plans, among other responsibilities.

In line with their changing role, the survey results also indicate that in most of the cases the responsibility of ensuring compliance is with the Board of Directors.

It is important to know that it is the management which is responsible for complying with the provisions of the Sarbanes-Oxley Act and specifically with section 404. Management may consult the legal counsel, independent auditors, and other professionals in meeting these obligations satisfactorily.

The respondents in our survey (88 percent) have also indicated that the responsibility for ensuring compliance with the new regulations (under SOX/ clause 49) rests internally within the organisations.

Effectiveness of SOX/ Clause 49

SOX requires the management of an organisation to evaluate the effectiveness of internal controls over financial reporting. Similarly under Clause 49, the CEO or the Chief Compliance Officer is expected to certify that the company is in compliance with all the applicable rules, laws and regulations required of a listed organisation.

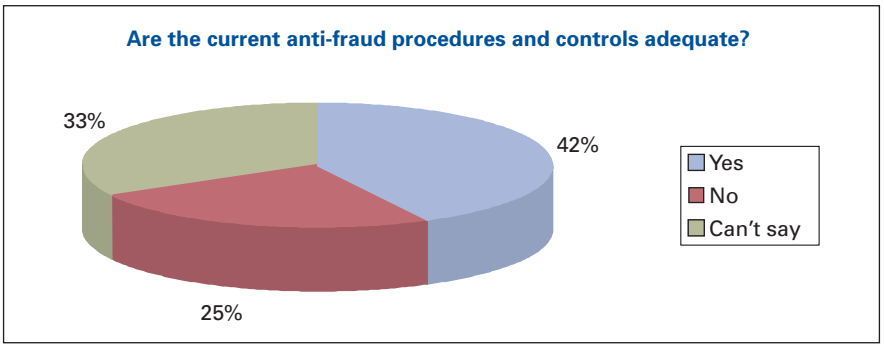
Majority of the respondent acknowledged that SOX/ Clause 49 have had an impact in controlling fraud or mitigating fraud risk.

Understanding and ensuring compliance with SOX or Clause 49 can be a formidable task, since, both of these have set out complex requirements for which organisations need significant commitment in the form of resources and time.

Even though, the implementation of the regulatory requirements is an expensive and a time consuming proposition, the results of our survey indicate that a majority of the respondent acknowledged that SOX/ Clause 49 have had an impact in controlling fraud or mitigating fraud risk.

Adequacy of current anti-fraud procedures and controls

In our survey, 25 percent of respondents indicated that their current anti-fraud procedures and controls are not adequate.



It is imperative for a company to establish adequate anti-fraud controls (in general anti-fraud programmes and controls are those programmes and controls that management establishes to prevent and detect fraud). This would include "company level controls" for which fraud prevention or detection is a component objective, e.g., the audit committee, code of conduct and hotline, and "process level controls" for which fraud prevention or detection is a primary objective, e.g., technology in the procurement process to detect fictitious vendors or component objective, e.g. bank reconciliations.

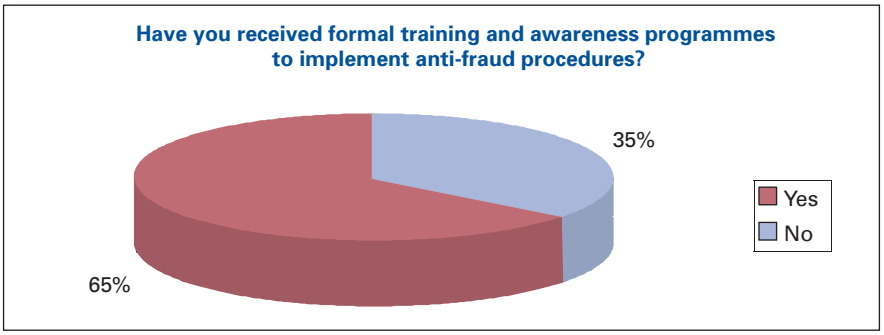
An auditor is expected to evaluate all controls specifically intended to address the risk of fraud that has a possible likelihood of having a material effect on the company's financial statements.

Training and awareness programmes

It was observed through the survey that a majority of the respondents had not been imparted any form of training or awareness programme which would have assisted them during the implementation of the SOX/ Clause 49 requirements.

A majority of the respondents had not been imparted any form of training or awareness programme for implementation of the SOX/ Clause 49.

Only 35 percent of the respondents agreed that they had received some training on how to implement anti-fraud procedures and controls and out of these people, 63 percent indicated that these programmes were conducted once in a year.



An organisation needs to demonstrate that it has a robust response plan and effective controls in place to act as a deterrent and that it takes the issue seriously by acting decisively if it discovers fraud.

To achieve this objective effectively, it is important that the anti-fraud stance becomes part of the organisation's culture, and formal training and awareness programmes are held periodically to communicate and re-emphasise the importance of appropriate anti-fraud mechanisms.

Intellectual Property

While most of the respondents considered their control mechanism to be average, almost one in every five felt that there is a scope for improvement.

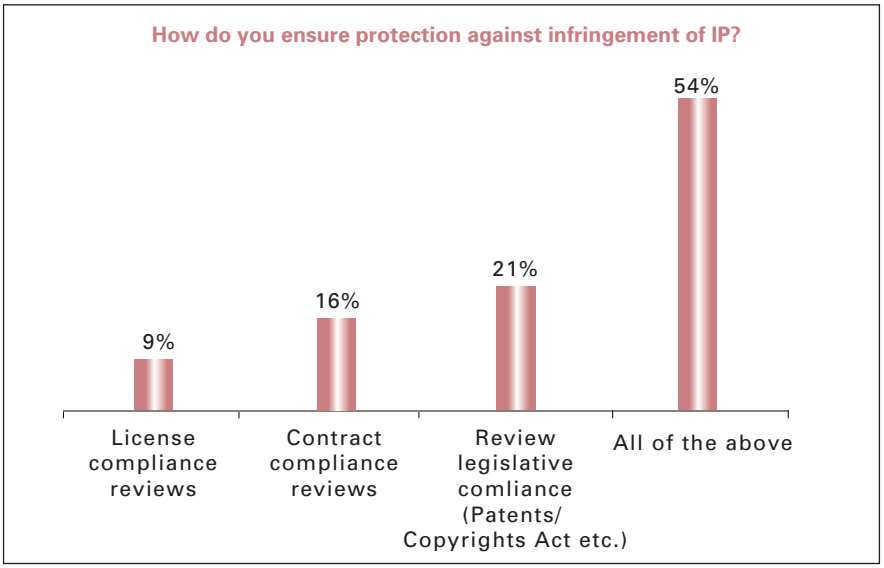
The intangible nature of Intellectual Property (IP) more often than not becomes the cause of its management and measurement being forgotten or even ignored, resulting in lost revenue, missed opportunities, and increased exposure to competitive threat or even litigation. Organisations have to address the challenge of building, utilising and protecting the value of the IP they own, use or have developed.

The exponential increase in the rate at which patents are being applied for/ issued, as well as the growing recognition of the value of IP is generating risks for companies across industries. In light of this observation it was only imperative to try and bring about an understanding on how organisations secure their IP.

The respondents were asked to comment on how they ensure protection. The options provided to them were:

- Through license compliance reviews
- Through contract compliance reviews
- Through review legislative compliance (Patents/ Copyrights Act etc.)

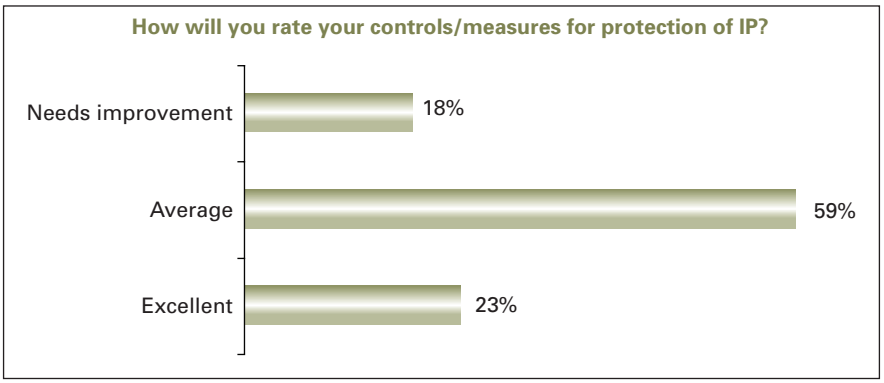
It was observed that 68 percent of the respondents owned some kind of an IP and of these, a majority of the organisations undertook reviews to safeguard their IP.



Effectiveness of controls/ measures

An important concern and priority for most organisations today is control and the measures which facilitate an effective control environment. Organisations need to be proactive about safeguarding IP and they need to ensure that revenues (if any) and rights are adequately protected. There is an imperative need to focus on ensuring compliance with contractual terms in areas such as IP, royalty and licensing.

Our survey results indicate that while most of the respondents considered their control mechanisms to be average, almost one in every five felt that there is a scope for improvement.



Typically, since financial arrangements rely on the "self-reporting" mechanisms, there may be frequent disagreements on the amounts which are payable/ receivable. KPMG's experience is that at least 70 percent of the self-reported statements are incorrect because of misreporting. The reasons for this misreporting could vary from misunderstandings to mistakes and occasionally fraud; however they all have a direct bearing on the organisation and could have severe impacts.

All of this highlights that there is an absolute necessity for an organisation to enhance its controls over IP, which in turn could lead to various benefits such as better management of contracts and licences potentially leading to improved business relationships; an improved cash realisation and income generation and finally a stronger competitive position.

Outsourcing/ Background checks

28 percent of the respondents have witnessed a fraud committed by outsourcing vendors. Almost 78 percent of the respondents acknowledged the need to undertake a background check on the third parties who may have access to the sensitive information.

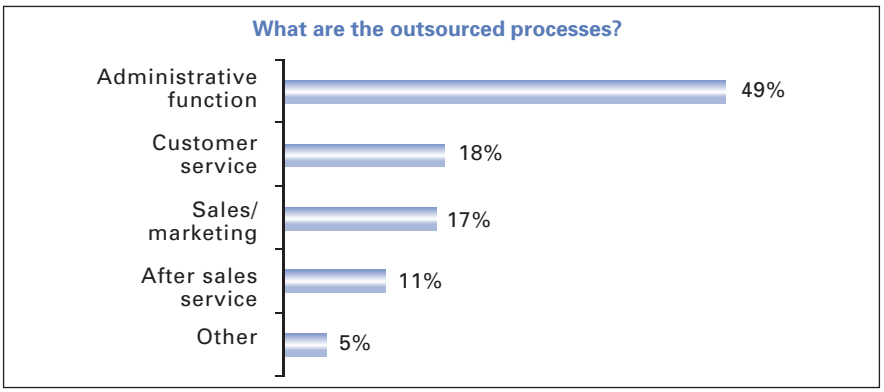
Outsourcing

The ever increasing complexities of work coupled with fierce competition and advancements in information and communication technologies have resulted in the emerging global reality of offshoring. To meet this new challenge and make a success out of it, Indian firms need to reposition themselves up the value chain and demonstrate effective risk management.

Organisations are moving their work processes to places where they can be managed more efficiently and effectively and unlike the popular belief costs may not be the sole criteria for this move. Offshoring objectives have now moved a long distance from achieving cost and quality advantages to focussing on mainstream business advantages of value creation and risk management. Building on the success of offshore services and contact centre offshoring, the global delivery structure now encompasses transaction processing and analytics.

With customers becoming more demanding of strong governance processes and meaningful performance metrics, suppliers will need to function as reliable utilities aligned to customer requirements. New concerns relating to confidentiality of data, quality of service and infrastructure and adherence to regulatory requirements are adding new dimensions to the already complex delivery model. These new operating realities combined with rapid growth are testing the managerial and operating capabilities of all stakeholders.

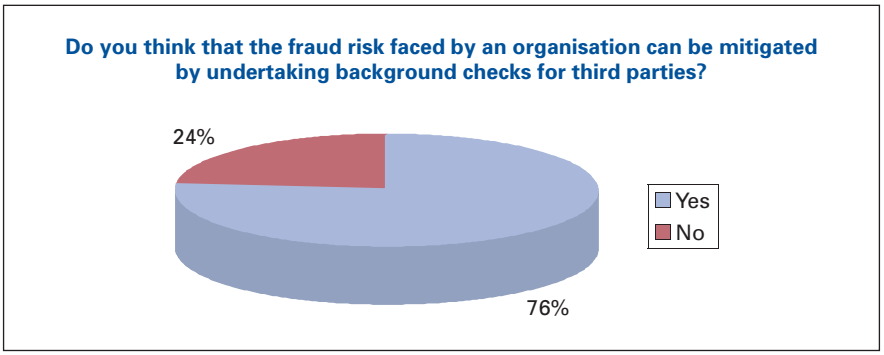
It was observed that 73 percent of the respondents were outsourcing work. Of these, nearly 49 percent of the respondents had outsourced an administrative function, followed by customer service at 18 percent and sales/ marketing at 17 percent.



Further, other functions being transferred are increasingly higher up the value chain, such as call centres, after sales service and customer account management.

Outsourcing not only involves the geographical transfer of jobs, but also the exporting of associated risks related to the integrity of employees, third party service providers or joint venture partners.

This is evident from the results of the survey which indicate that a fair portion (28 percent) of the respondents has witnessed a fraud committed by outsourcing vendors. Almost 76 percent of the respondents acknowledged the need to undertake a background check on the third parties who may have access to sensitive information.



Knowledge and adequate control systems can act as the key for an organisation to prevent fraud, however, organisations often take decisions to appoint potential suppliers and business associates without carrying out adequate diligence.

Relationship building is crucial to an organisation's success in today's competitive market; however, entering into any kind of relationship without an appreciation of the possible pitfalls can expose an organisation to the potential risk of fraud. This fact is further compounded since organisations often need to operate in unfamiliar territories or with inadequate knowledge of the background of the employee/ prospect and the reputation or ability to conduct business of their potential business partners. Many a times the organisation or the management tends to ignore the track record and reputation of the prospect while focussing only on the potential financial gains.

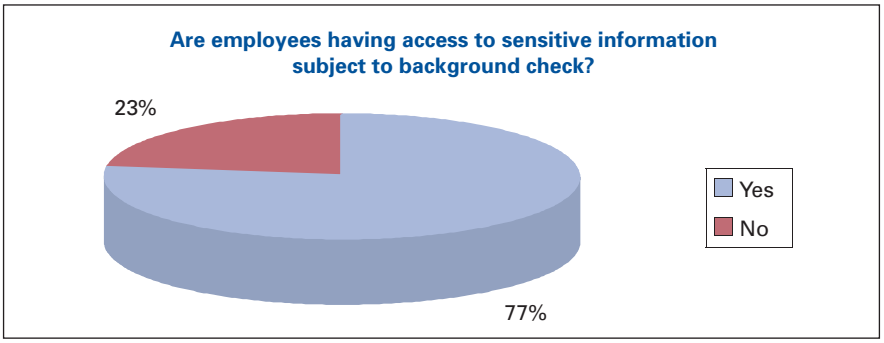
To mitigate any fraud risks faced while dealing with third parties, organisations should attempt to ascertain the credibility of the information provided by potential vendors.

Background checks for prospective employees

In today's market, more often than not, organisations may get tempted to fill up vacancies with the first applicant who meets all requirements. However, taking time to find the right candidate for the job should include a pre-employment screening that can facilitate an organisation in minimising the threat of fraud or misconduct. Recent incidents relating to inadequate control mechanisms and leakage of customer data have tested the managerial and operating capabilities of outsourcing firms in providing a secure solution framework that also focusses on fraud prevention.

There is a considerable amount of concealment of correct information by the potential job applicant which could not be uncovered by organisations.

The results of this survey indicate that a majority of the organisations (77 percent) realise the importance of conducting background checks for employees who have access to sensitive information or restricted areas.

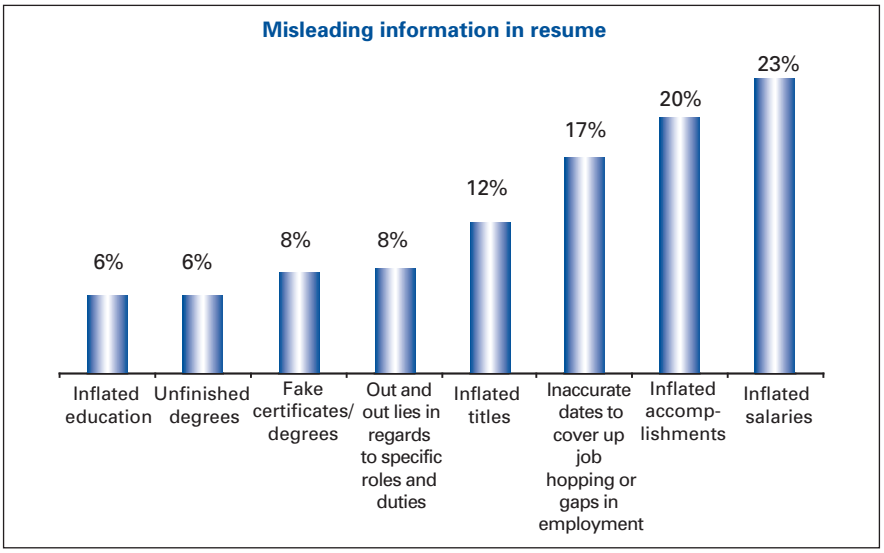


In more recent times, the BPO industry has witnessed a large number of high profile and well planned frauds where the sole reason was established to be the employee misconduct. This coupled with the unusually high rates of attrition in the industry forced the National Association of Software and Service Companies (NASSCOM) and the BPO sector (in association with National Securities Depository Limited) to create a comprehensive employee registry. This is one of the first steps towards establishing a better check on the employee's background and history.

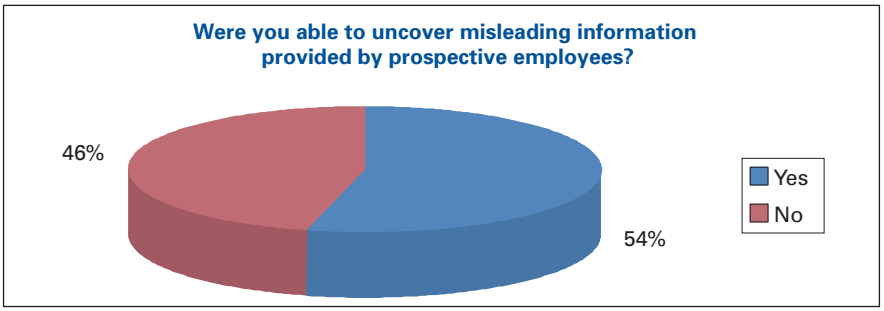
This registry will attempt to provide a medium which helps strike a balance in maintaining the privacy of employee data and at the same time reinforce the need for companies to check the backgrounds of the staff they hire. Initiatives like these facilitate the conduct of background checks on employees, thereby reducing the risk of fraud related activities. This exercise will result in validation of personal details, address, qualification, employment history, photograph, and signature.

We were interested in finding out the extent and kind of misleading information prospective employees generally include in their resume. The respondents highlighted four main areas of incorrect information among others:

- Inflated salaries (23 percent)
- Inflated accomplishments (20 percent)
- Inaccurate dates to cover up job hopping or gaps in employment (17 percent)
- Inflated titles (12 percent)



The data suggests that there is a considerable amount of concealment of correct information by the potential applicant; further the survey results also help in inferring that a large proportion of respondent organisations (46 percent) were not able to uncover such misleading information. This reflects on the inadequacy and incomplete nature of control mechanisms that corporate India is living with.



Organisations around the world are waking up to the concerns about security and confidentiality of assets and information within organisations. For example if a person with a criminal record is employed, he could pose a threat to an organisation's existing employees, customers and property.

Many employers discover rather late that they have hired violent offenders and persons with a history of crime involving theft, embezzlement or fraud in various forms. Employers need to start undertaking pre-employment screening to discover important information that can influence the hiring decisions. The check serves as a foundation for a more secure and stable future for organisations and a greater emphasis needs to be laid on making it a part of the routine recruitment process.

Cyber security – an emerging need

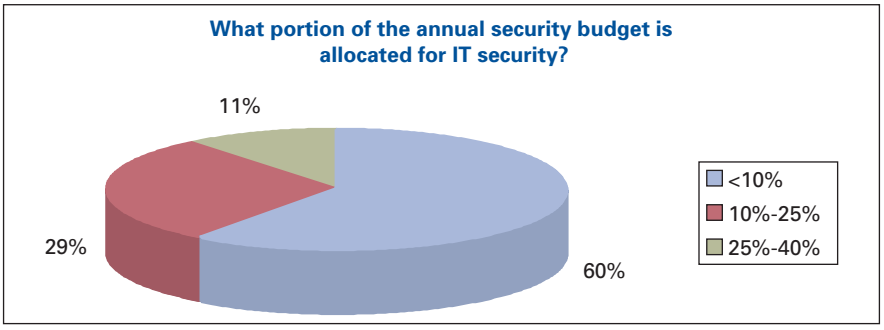
The development of new threats has been faster than what the IT world could ever imagine or even come up with terms to describe them.

In today's age of convenient and faster communication there is an increasing technological dependence, which makes cyber safety a critical concern for organisations. Recent incidents relating to cyber crime have not just increased the vulnerability of various socio-economic constituents, but also brought forth the need for better managerial and operating capabilities of our legal framework in stopping this growing menace.

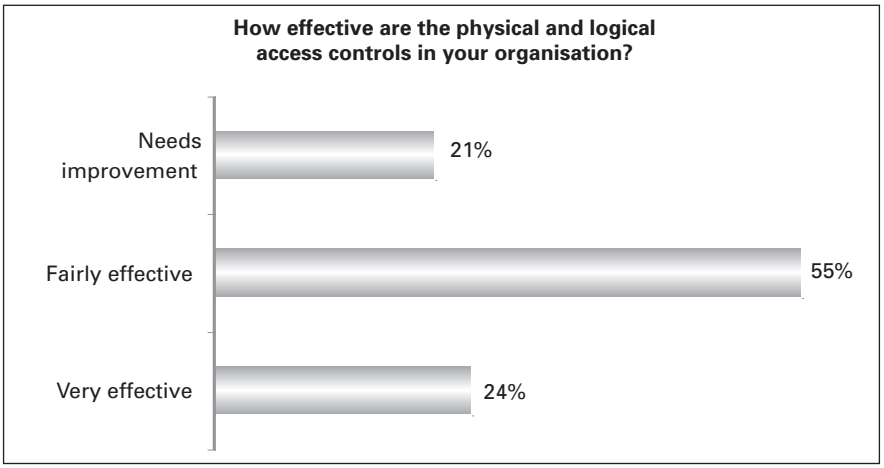
Over the last few years, the frauds within the IT world have not only increased in occurrence but also managed to change its forms. The development of new threats has been faster than what the IT world could ever imagine or even come up with terms to describe them (e.g. morphing, phishing, pharming, spear phishing). The distinction between the various types of threats is getting more and more emulsified which is why there was an increasing emphasis on secrecy and stealth, making spyware one of the biggest threats that modern businesses now face.

IT security budget

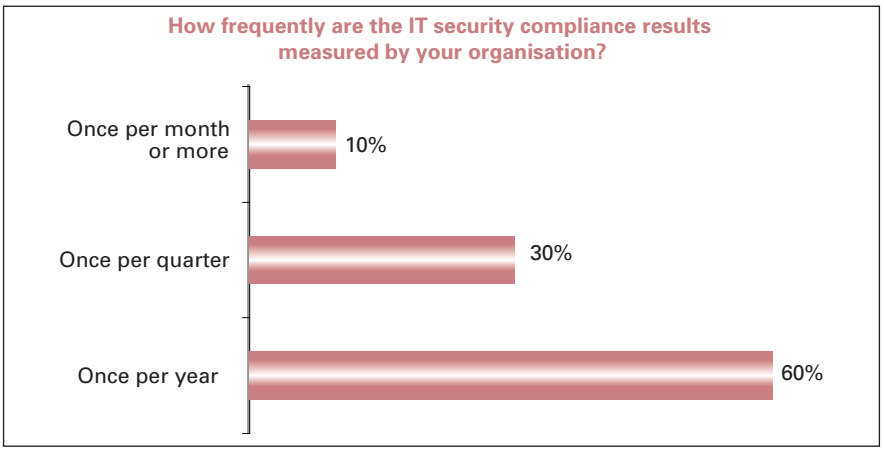
The survey brought out some rather interesting observations with 60 percent of the respondents having allocated less than even 10 percent to total IT security spend. On an overall basis about 89 percent of the respondents had allocated less than 25 percent of their annual security budget to IT security.



With respect to the effectiveness of physical and logical access controls in organisations, the survey revealed that while 24 percent were of the opinion that they had very effective controls, the remaining 76 percent opined that their control system was either fairly effective or required improvement.



It was essential to understand the frequency of measuring the IT security compliance results; and when asked, 60 percent of the respondents revealed that they conducted such reviews only once a year. A very small percentage of respondents, about 10 percent, conducted these compliance reviews more than once per year.



Information technology when correctly implemented and used effectively can be a boon for any organisation and the need for security of IT systems should be a key management concern in any business environment.

It is indispensable for an organisation to manage these risks and assess, design, implement and maintain security and controls that help mitigate such risks. This also provides an assurance to the management on the confidentiality, integrity and availability of information.

Absence of an IT security policy indicates a lack of recognition by senior management of the need for security in their organisation and could have deleterious consequences.

A well-developed IT security policy document equips the organisation with an objective tool to assess the criticality of its information assets, determines the extent of security required and assigns appropriate access to internal and external agencies.

Experience of fraud in organisations

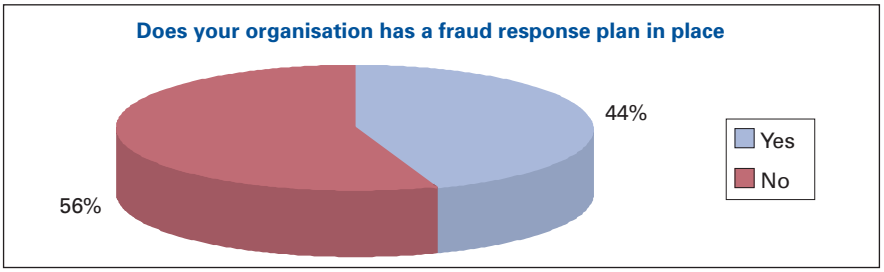
More than half of the respondents (about 56 percent) confirmed that they did not have any formal fraud response plan in place to minimise the impact of fraud.

Fraud does have its impact in an organisation and in some cases it may have long term repercussions and prove to be a handicap for a company's reputation thus affecting its business and other areas. In order to develop a clear insight on the impact of fraud in the organisation, we asked specific questions related to instances of fraud, vulnerable areas, detection, investigation and action taken by the organisations.

Existence of a fraud response plan

A fraud response plan details how to handle a suspected fraud incident, how to manage subsequent risk operations and further how to deal with the investigation which implies deciding on specifics such as who needs to be told and who will investigate?

More than half of the respondents (about 56 percent) confirmed that they did not have any formal fraud response plan in place to minimise the impact of fraud. This is a considerable percentage, considering that it is a crucial requirement for any organisation to safeguard itself from potential fraud or misconduct.



It is critical that companies have a fraud control plan. Such a plan amongst other things should comment on:

- Responsibilities in case of a fraud
- Escalation mechanisms
- Access restrictions
- Securing evidence (data and information)
- Involving legal counsel
- Involvement of specialists
- Reporting for compliance
- The investigation

Occurrence of fraud

The survey respondents were asked if they were aware of any fraud that had occurred in their organisation in the past one year and the results were quite interesting. Almost 39 percent of the respondents indicated that their organisation had been affected by fraud while the majority replied in the

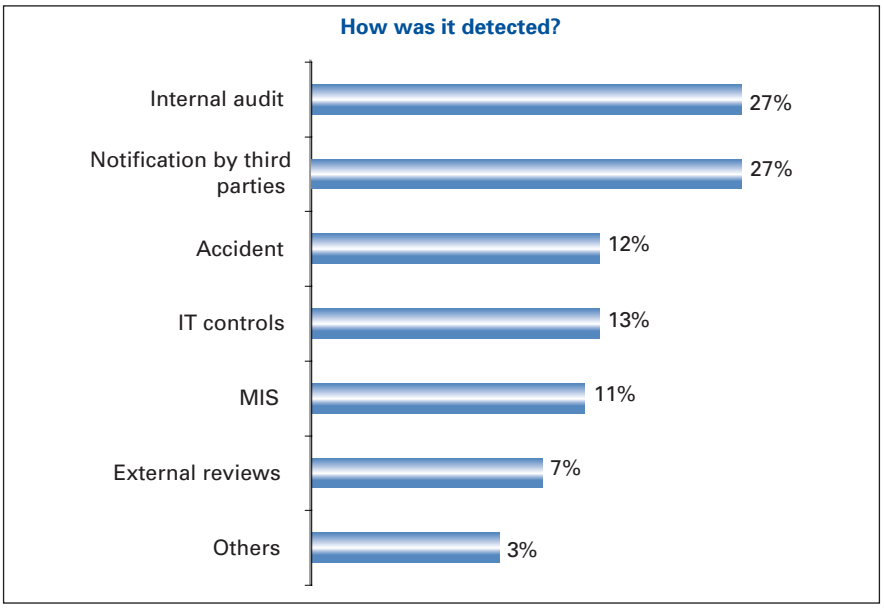
The majority of the frauds reported by respondents were identified either through the organisation's own internal audit department or were notified by a third party.

negative. However, this still is quite a big percentage of organisations being affected by recent frauds.

How was it detected?

It is critical to establish the source and the medium through which the fraud was identified. The survey showed that the majority of the frauds reported by respondents were identified either through the organisation's own internal audit department or were notified by a third party (both were at 27 percent). This suggests that an organisation's fraud control programme should allow external parties to report allegations or suspicions of fraud.

A fair portion of the respondents also indicated that the fraud was detected by internal IT controls which had been put in place (13 percent) by the organisation. This is an interesting observation considering that the respondents felt that the maximum threat perception was from lack of internal controls. This just sends out a clear message that organisations need to perhaps build preventive and detective controls into the IT systems to mitigate the fraud risk.

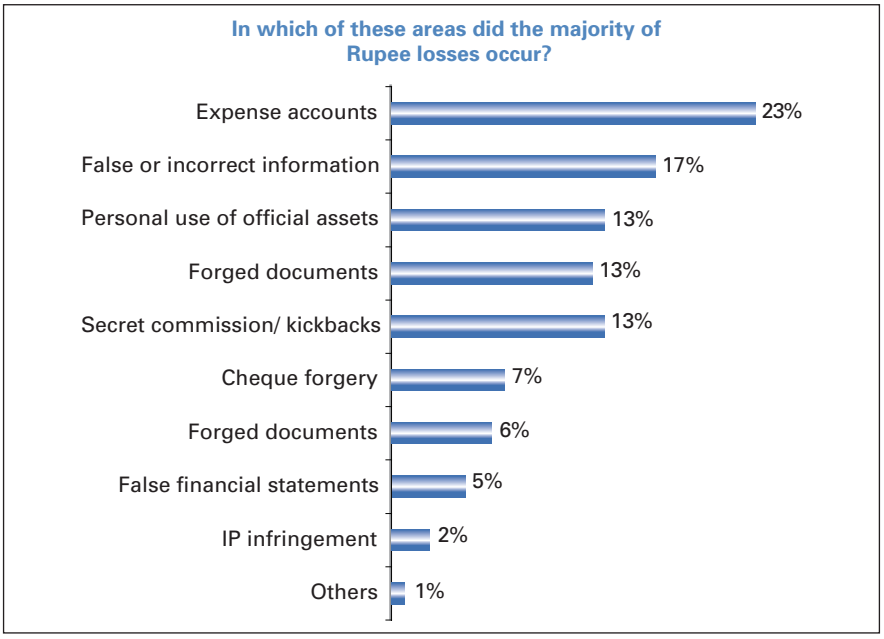


Expense account continue to be the most susceptible area to fraud, followed by false false or incorrect information, personal use of assets and forged documents.

In which areas did the majority of rupee losses occur?

In the surveys conducted by us in the previous years, expense accounts had always figured on the top of the list when it came to the most critical and expensive type of fraud. The other areas which were also thought as a common sight for frauds by respondents included secret commissions, forged documents, false or incorrect information and misappropriation of funds.

The trend in the current years was observed to be considerably similar. Expense accounts continue to be the more critical medium and were followed by false or incorrect information, personal use of assets and forged documents.

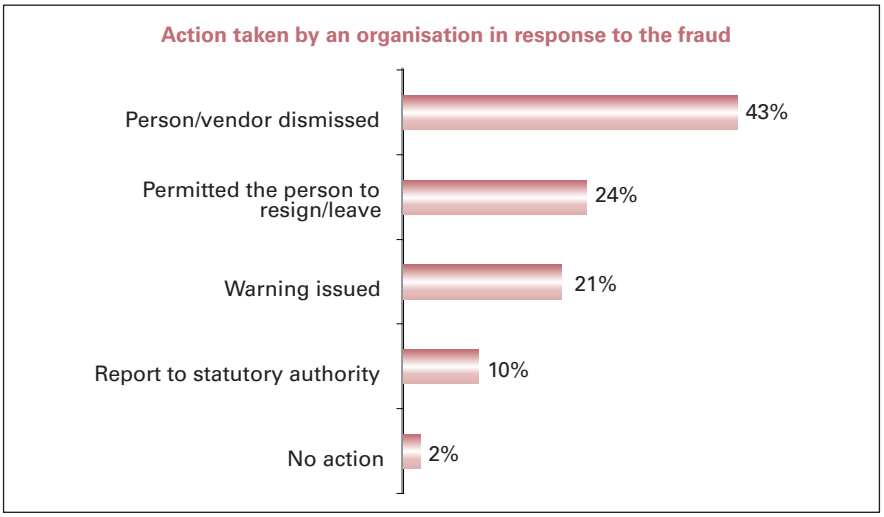


Action taken in response to the fraud

It is important that a careful consideration of the costs, benefits and implications of all possible actions is conducted while dealing with fraud incident. In situations involving fraud it is essential for senior management to set the appropriate tone critical to the creation of an ethical environment and thus facilitating effective and efficient management of fraud risks in the organisation.

Our own experience during investigations has been that more often than not, fraudsters have been either dismissed or have been allowed to leave/ resign. We asked the respondents what actions did they take to deal with the fraud incidents and the most common response provided by the respondents was to dismiss the vendor/ person perpetrating the fraud (43 percent). This was followed by permitting the person to leave/ resign (24 percent) and issuing a warning (21 percent) to the perpetrator.

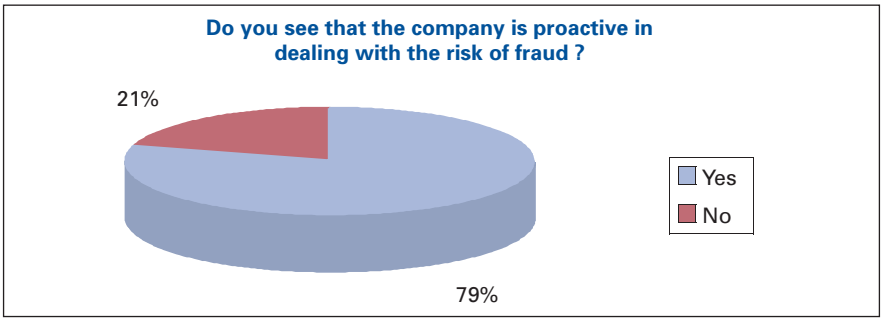
There is a shift in the attitude of organisations towards fraud, and there is a distinct move from being reactive to being a lot more proactive about fraud.



Proactiveness of the organisation in dealing with the risk of fraud

Our experience over the years has shown a relative shift in the attitude of organisations towards fraud, and there is a distinct move from being reactive to being a lot more proactive about fraud.

This fact is apparent from the responses of the survey with majority of the respondents (79 percent) considering their organisation as being proactive in dealing with the risk of fraud.



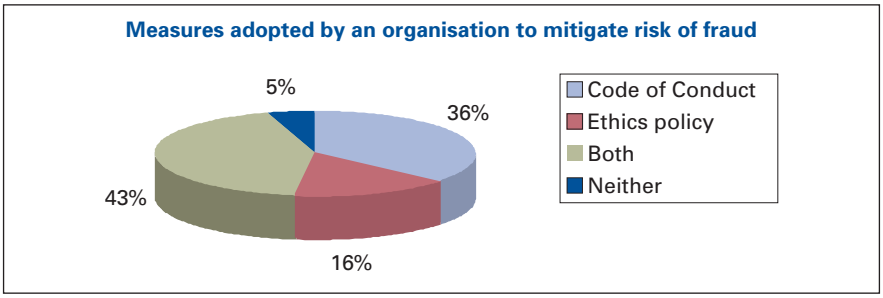
Responsibility of fraud control

Most of the organisations either have a code of conduct or an ethics policy in place as a proactive measure to mitigate risk of fraud.

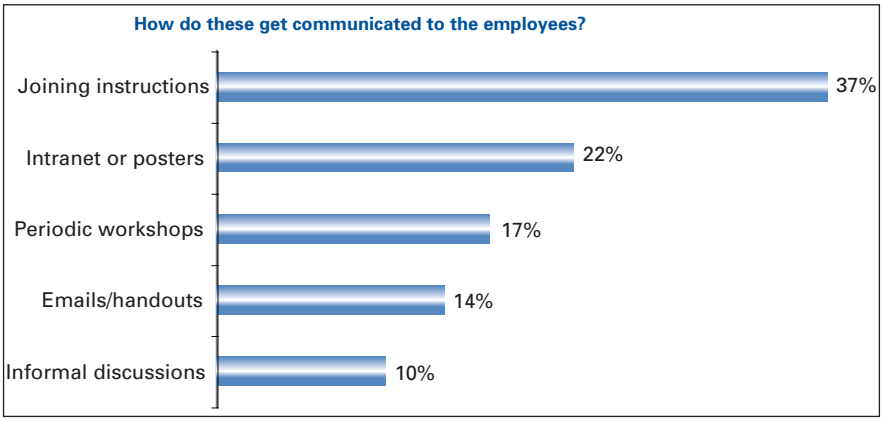
Risk is inherent in business processes and emanates from actions taken in pursuit of objectives and from changes in the external environment. An organisation, while aiming at meeting the expectations of its shareholders, sometimes exposes itself to certain level of risk. However, it is essential to understand that the key to risk management is effectively balancing risk and control.

The corporate community around the world has learnt their lessons by experiences of some major corporate failures. Regulatory requirements expect organisations to have effective risk management practices. The corporate community around the world has acknowledged this fact with India not being too far behind.

The survey respondents were asked about proactive measures being employed in their organisation to mitigate fraud risk and 36 percent of the respondents had a code of conduct while 16 percent had an ethics policy in place. 43 percent of the respondents replied that they had both of these in place in their organisation.



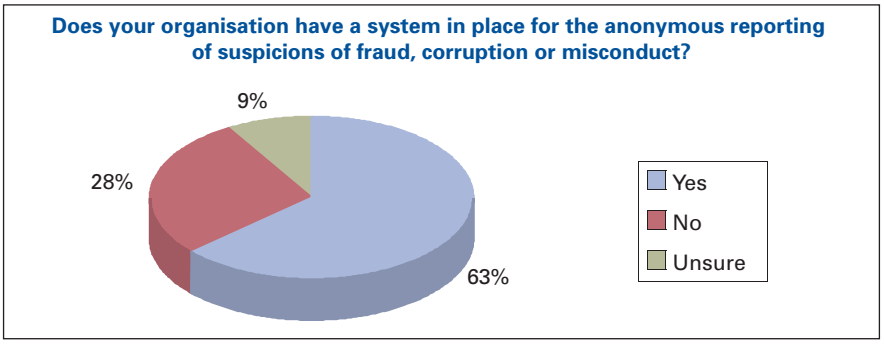
By means of further queries it was established that in 37 percent of the cases the organisation was communicating these policies to its employees as part of the induction programme. The other formal methods which were being used at the post joining stage included policy information being made available on the intranet or through posters, emails/ handouts and periodic trainings.



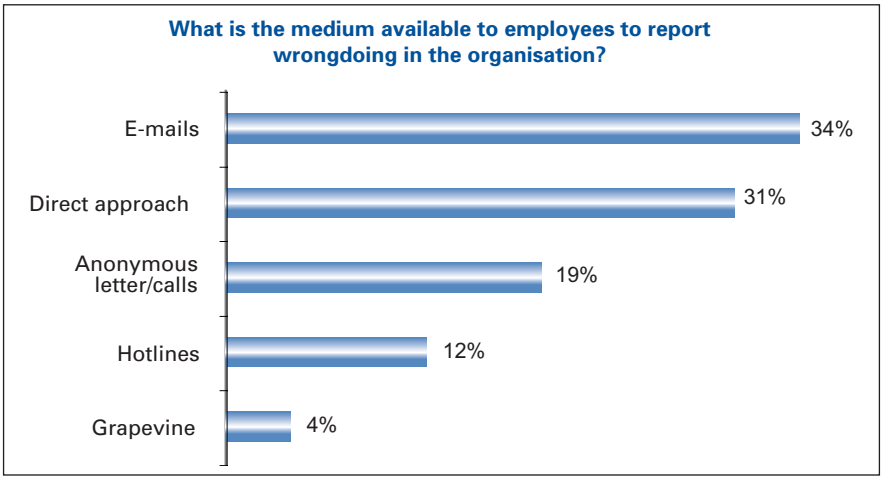
It is critical that such policies and expectations from an employee are communicated at the time of joining and then it needs to be reiterated periodically through regular communication and training programmes.

System/ medium for reporting of fraud or misconduct suspicions

It was observed through the responses that a significant portion (37 percent) of the respondents agreed that either they did not have any system in place for reporting of suspicions of fraud, corruption or misconduct or they were not sure of the same.

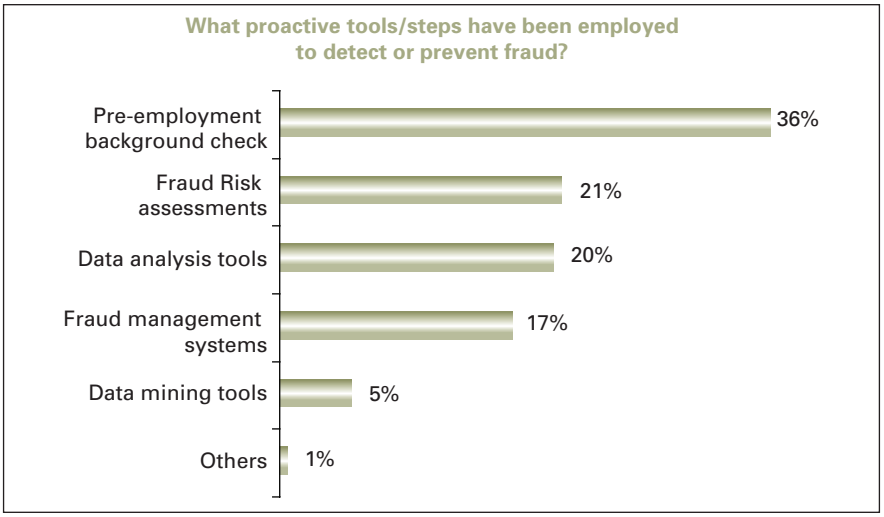


The majority of the respondents indicated that they would report suspicion of a fraud using e-mails (34 percent), however a direct approach (31 percent) and anonymous letters/ calls (19 percent) were also the mediums which were favoured by whitle blowers.



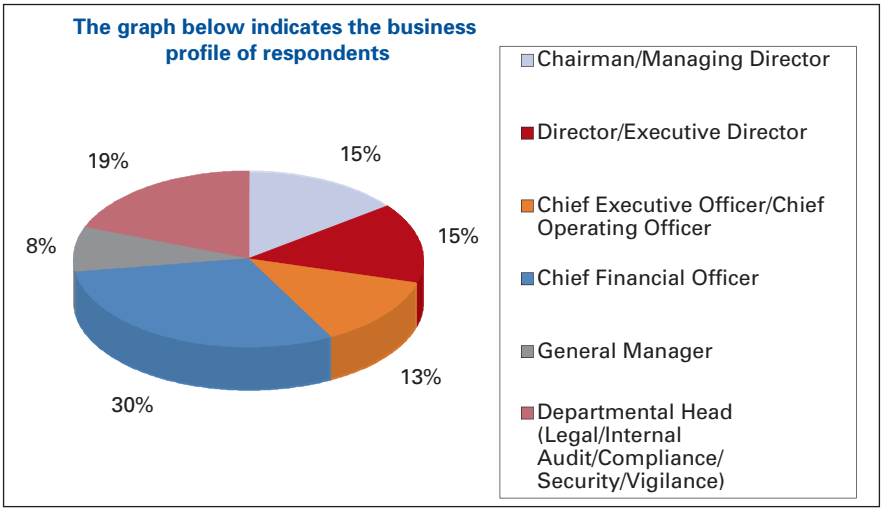
Proactive tools/ steps employed to detect or prevent fraud

We had asked the respondents about the kind of proactive tools employed by them in order to detect/ prevent frauds in their organisations and the results indicated that the maximum emphasis (36 percent) was given to pre-employment background check. A significant number of respondents also employed fraud risk assessments (21 percent) and data analysis tools (20 percent) as proactive steps to detect fraud.

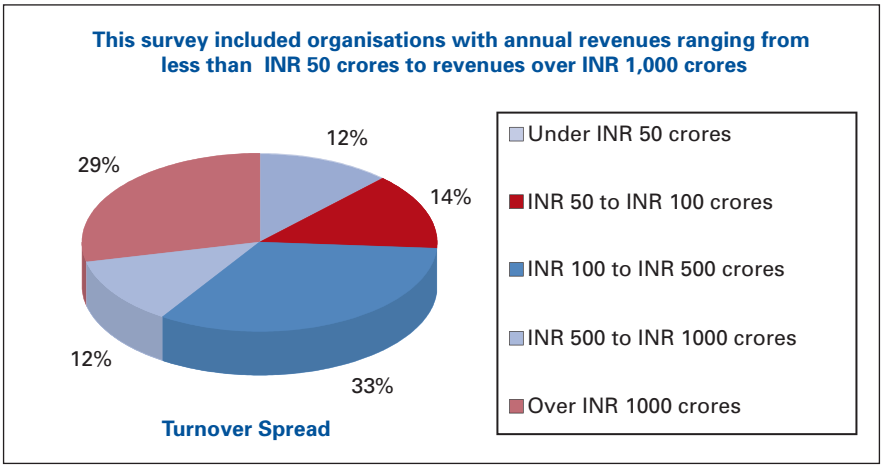


Profile of the respondents

The graph below indicates the business profile of respondents

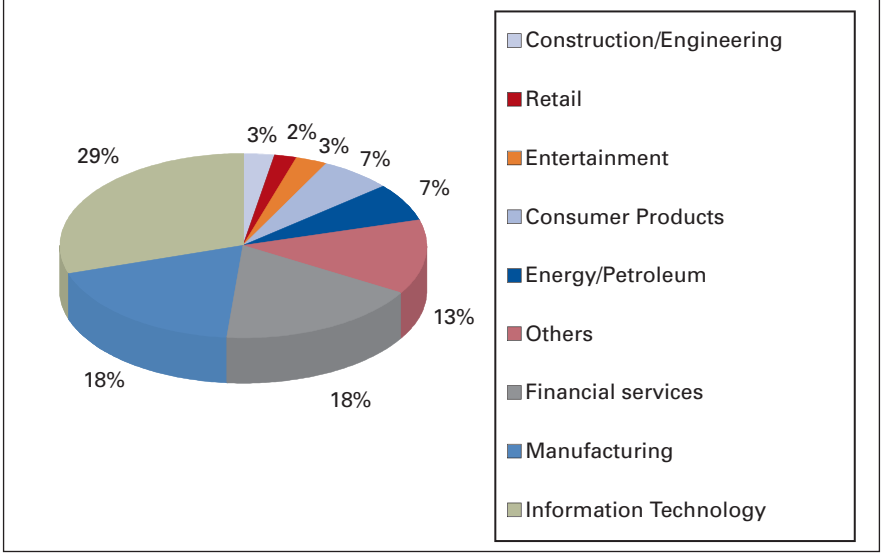


This survey included organisations with annual revenues ranging from less than INR 50 crores to revenues over INR 1,000 crores



Turnover Spread

Industry sector profile represented by respondents' organisations



in.kpmg.com

For further information about this survey or the services offered by KPMG Forensic, please contact us on:

Mumbai
KPMG House
Kamala Mills Compound
448, Senapati Bapat Marg
Lower Parel
Mumbai 400 013
Telephone: +91 22 3989 6000
Fax : +91 22 2491 3132

Delhi
4B, DLF Corporate Park
DLF City, Phase III
Gurgaon 122 002
Telephone: +91 124 254 9191
Fax : +91 124 254 9101

Bangalore
Maruthi Infotech Centre
11/1 & 12/1, East Wing, II Floor
Koramangala-Inner Ring Road
Bangalore - 560 071
Telephone: +91 80 4176 6000
Fax: +91 80 4176 6999

Chennai
II Floor, Westminster
108, Dr. Radhakrishnan Salai
Mylapore
Chennai 600 004
Telephone: +91 44 2847 3911
Fax: +91 44 2847 3912

Hyderabad
II Floor, Merchant Towers
Road No. 4, Banjara Hills
Hyderabad 500 034
Telephone: +91 40 2651 0060
Fax: +91 40 2335 0070

Kolkata
Park Plaza
Block F, Floor 6
71 Park Street
Kolkata 700 016
Telephone : +91 33 2217 2858
Fax: +91 33 2217 2868

Pune
703, Godrej Castlemaine
Bund Garden
Pune 411 001
Tel: +91 20 3058 5764/ 65
Fax: +91 20 30585775