

Fraud and corporate governance: Changing paradigm in India

A report based on India fraud survey 2012



Introduction


India is an emerging market, which is witnessing rapid economic growth. But the spate of scams unearthed in the last few years has raised anxiety in the minds of foreign investors, who are looking to be part of the Indian growth story, but are wary of fraud, bribery and corruption risks.

On looking beyond our borders, we observe that the increasingly multi-directional flow of trade and investment has created a polycentric world in which opportunities, capabilities and competition are spread broadly across multiple spheres of influence.¹ In addition, there are increasing risks and challenges, as governments around the world introduce anti-corruption legislation such as the US Foreign Corrupt Practices Act (FCPA) 1977 and the UK Bribery Act 2010, which have extra-territorial jurisdiction. Bribery and corruption continues to be the biggest challenge in the corporate world, and the risk is compounded by increasing enforcement of regulations and stricter penalties.

Indian policy makers are taking robust steps to increase the confidence of investors – corporate and public. In the recently concluded Parliamentary sessions, two important bills were introduced – the Prevention of Bribery of Foreign Public Officials Bill and The Anti-Corruption, Grievance Redressal and Whistle-blower Protection Bill. In addition to this, ratification of the United Nations Convention against Corruption (UNCAC) by the Government this year has helped India demonstrate its commitment to good governance. In another significant development, the Government is working on the Lokpal Bill, which aims to create stricter regulations and has given more credibility to its fight against bribery and corruption. We hope these steps will help the country recover from the setbacks it has faced and that investors with a long-term view will focus on the opportunities being offered in the domestic market.

This year, we have made an attempt to take our study beyond the fraud scenario to understand the profile of a fraudster. According to the profile created by the majority of the respondents, a typical fraudster is an internal male employee, who is in his 30s, is far from the age of retirement and is an





average performer in middle management from the procurement or sales department. This profile description does not come as a surprise, with increasing consumerism and the desire for instant gratification driving employees to commit fraud against their companies. However, although insider threats are easy to understand, they are hard to detect as compared to external ones.

According to our respondents, external perception of their company is very important – more than half of them feel that damage to an organization's reputation is the greatest collateral damage caused by fraud. This fear also stems from the fact that damage to a company's reputation can result in loss of revenue or destruction of shareholder value, even if it is not found guilty of a crime. One of the possible causes for the increasing trend of fraud being committed by employees could be corporate reluctance to seek legal recourse against employees.

Today, we see a number of companies wanting to incorporate proactive fraud risk management in their companies as compared to a year ago. This is an encouraging sign, which indicates a brighter future for corporate governance in India.

We hope you gain some useful insights from this report, and it helps you to address challenges and risks faced by your business.

We take this opportunity to express our gratitude to the people and organizations who took time to respond to our survey. The report and the findings would not have the same value without the support of these respondents and all those who made the survey successful.



Arpinder Singh

Partner and National Director
Fraud Investigation & Dispute Services
Ernst & Young Pvt. Ltd.



In this report

Executive summary	2
What lies beneath	4
Section 1: Fraud scenario in India – ground reality	6
Cost of fraud – more than monetary	7
Discovery of fraud – methodical and accidental	7
Current practices – inconsistent with globally accepted norms	8
Growing greed – profile of a fraudster	9
Section 2: Areas of concern	10
Data and information theft - managing insider threat	11
Management's overriding controls	11
Supply chain leakage facilitating counterfeiting in consumer product industry	12
Bribery and corruption - the perpetual challenge	13
Section 3: Changing regulatory landscape	18
Section 4: Tools for fighting fraud.....	20
Role of technology	21
Whistle-blowing.....	23
Fraud response plan.....	24
Third party due diligence	24
Independent directors – a strong influence.....	25
About the research	26

Executive summary

This study aims to understand how businesses have coped with increasing fraud and corruption risk last year, what the emerging fraud risks in the industry are and the measures taken by various organizations to mitigate these risks.

Some key highlights of the study

► Increasing incidence of fraud

Nearly three-fifths of the respondents said that their companies have been subjected to fraud during the course of last year. Moreover, with the growing use of technology in business operations, instances of technology-led fraud has also increased significantly. Since most of the traditional processes in a company, e.g., accounting, procurement, etc., are moving to IT-based processes and systems, and may eventually move to cloud computing, so is fraud in these areas. This is posing a major challenge for organizations today².

► Top five fraud risks

1. Data or information theft and IP infringement
2. Bribery and corruption
3. Fraud by senior management and conflict of interest
4. Vendor fraud or kickbacks.
5. Regulatory non-compliance

Data or information theft has emerged as a new threat in the evolving risk landscape due to the proliferation of IT, giving rise to issues relating to privacy and data protection.

► Changing profile of a fraudster

According to most survey respondents, “He is an internal employee of a company, who is in his 30s and is far from retirement. He is in the middle management cadre, working in the procurement or sales department.” With increasing

consumerism, there is a shift from the “need” to “greed” as a motive for committing fraud. And today we are seeing a trend where younger employees are increasingly committing fraud to support a lifestyle that is not commensurate with their incomes. This appears to be in line with the increasing consumerism in India.

► Lack of action against the fraud perpetrator

Companies are reluctant to take legal recourse against employees responsible for committing fraud. Only 35% of the respondents said that their company takes any disciplinary action against unscrupulous employees. One reason for this could be that companies fear possible damage to their reputation if news about the fraudulent incidence leaks into the public domain.

► Significant impact of fraud

Loss of reputation emerged as the biggest and severest collateral damage caused by fraud. External perception is highly valued by companies, since damage to their reputation can result in loss of revenue or destruction of shareholder value, even if they are not found guilty of having committed a crime.

► Continuing bribery and corruption risk

Bribery and corruption continue to be a perpetual challenge for corporate India.

1. **Level of awareness:** Around 70% of the respondents were aware of the Prevention of Corruption Act 1988. This is not surprising in view of recent scams and subsequent media and public activism. However, with more than 75% of the respondents working in multinational corporations (MNCs), less than 50% are aware of global anti-graft legislations such as the US FCPA and the UK Bribery Act.
2. **Rationale for bribery:** Kickbacks are given to win or retain business, to obtain approvals from government agencies and to influence people to make favorable decisions.

2 Technology fraud: a changing world, Ernst & Young, 2011



3. **Common mode:** Cash and gifts are the most common mode of giving bribes.
4. **Factors facilitating bribery and corruption:** Nearly 40% of the respondents indicated that the inherent nature of the industry in which their companies operate is responsible for encouraging corruption; 34% of the respondents said that this is due to organizations having a “weak tone at the top.”
5. **Lack of enforcement of anti-corruption laws:** Around 33% of the respondents said that lack of an effective regulatory and compliance mechanism, and weak law enforcement are equally responsible for facilitating corruption.
6. **Fight against bribery and corruption:** Around 62% of the respondents are in favor of stringent disciplinary procedures and 73% said that companies should adopt a zero tolerance approach to bribery and corruption, e.g., by taking legal action against the perpetrators of fraud.

► **Weak anti-fraud measures**

Companies still rely on old traditional anti-fraud measures. Reliance on internal and external audit, and code of conduct is high. This seems surprising in today's environment, where fraudsters are using advanced tools and technology to perpetrate frauds.

Proactive fraud risk management: Need of the hour

Business leaders are aware of the need to address fraud risks, but lack of a comprehensive and integrated approach to fraud risk management continues to be a concern. Currently, companies take a “check-the-box” approach to fraud risk management, conducting isolated risk assessments, whereas the need of the hour is a cohesive but wider approach, aligned with the strategic business objectives of organizations.

Technology can play a larger role in fraud risk management. Another possible area that should be considered by companies in countering fraud risk is a whistle-blowing mechanism.

Changing regulatory scenario: Positive change

There is increased regulatory activism, and existing Acts are being amended and updated to address new and complex threats. Regulators are proposing more stringent standards for prevention, detection and reporting of fraud. For instance, the Government has proposed various measures to counter fraud risk in the Companies Bill 2011, which is slated to replace the Companies Act 1956. This is in addition to many current regulations such as Clause 49 of the listing agreement, Companies' (Auditor's Report) Order (CARO) 2003, which entrusts the responsibility of preventing corporate fraud to the Directors, CEO, CFO and auditors of a company.

The fact that around two-thirds of the respondents said that scams and corporate frauds were unearthed because of legislations such as the Right to Information Act (RTI) and Public Interest Litigation (PIL) speaks volumes about public awareness in India.

Globalization has added to the regulations to which companies need to adhere. Governments around the world, in an attempt to address bribery and corruption risks, have introduced anti-corruption legislation such as the US FCPA and the UK Bribery Act, which have extra-territorial jurisdiction.

Future outlook

More and more companies are taking cognizance of the changing regulatory scenario. We are seeing an increased focus on corporate governance. Also companies are increasingly now taking proactive measures against fraud, bribery and corruption.

What lies beneath³



According to more than three-fourths of the respondents, the incidence of fraud has increased in the country in this last one year.

Rapid-growth markets such as India have gained significant momentum due to their rising per capita incomes, favorable demographics and large populations. Most have come through the financial crisis with very little long-term damage and continue to have impressive growth trajectories. With economic growth projected to surpass 8% annually and the number of people in the Indian middle class set to treble over the next 15 years, domestic demand is expected to grow at a compound rate of 9.2% per year between 2010 and 2030. This places India in a favorable position to attract an increasing proportion of global foreign direct investments (FDI).⁴

Although India is on the expansion path of MNCs looking for high growth, recent fraudulent incidents reported by the media have made foreign investors wary of various hidden risks. They are faced with the dual challenge of achieving aggressive growth numbers and ensuring that in the process they are not violating any regulatory guidelines. The complex business environment, renewed regulatory activism and increasing use of technology have tipped the scale against corporate organizations that are hard-pressed to deliver business results in today's risk-prone scenario.

India struggles with corruption issues, perceived and real. According to the 2011 Corruption Perception Index (CPI), the country is ranked 95th out of 183 countries, and has scored less than in previous years – 3.1 on a scale of 0 to 10 where 0 stood for highly corrupt.⁵

Practical issues that companies may face in an emerging market such as India:

- ▶ Lack of availability of unique identification number and reliable rating data for entities or individuals

- ▶ Facing the challenges of bribery and corruption, particularly while working with local partners, who may have a different approach to conducting business
- ▶ Extensive use of cash or cheques, rather than electronic transfers, with the danger that these may be used to facilitate unethical business practices
- ▶ “Relatively weak governance” comprising one of the top challenges companies can face in the country

Corruption is often cited as one of the main challenges faced by India. The Government has taken steps to fight it by offering many of its services online, thereby reducing avenues through which corrupt officials can demand bribes. However, recent scandals have underlined the persistence of this problem.⁶

Despite the prevalence of bribery and corruption, legal and regulatory intervention, as well as increased attention being paid to this issue by corporate organizations, seems to be having a positive effect. The Government recognizes that bribery and corruption are detrimental for business and companies are taking corporate governance seriously and aligning their business strategies to reflect this. As a result, we are seeing a steady decline in this problem, although it is an ongoing process that will require continuous intervention from the Government and the corporate sector to make further progress.

3 “What lies beneath? The hidden costs of entering rapid-growth markets,” Ernst & Young Master CFO Series, 2011

4 Reaching toward its true potential, Ernst & Young’s 2011 India attractiveness survey.

5 Corruption perception Index 2011, Transparency International, December 2011.

6 Reaching toward its true potential, Ernst & Young’s 2011 India attractiveness survey.

Section 1:

Fraud scenario in India

Ground reality



In the survey, nearly three out five respondents revealed that their companies had been subjected to fraud during this last one year. Out of these respondents, around two-third said that it was exposed because of whistle-blowing.

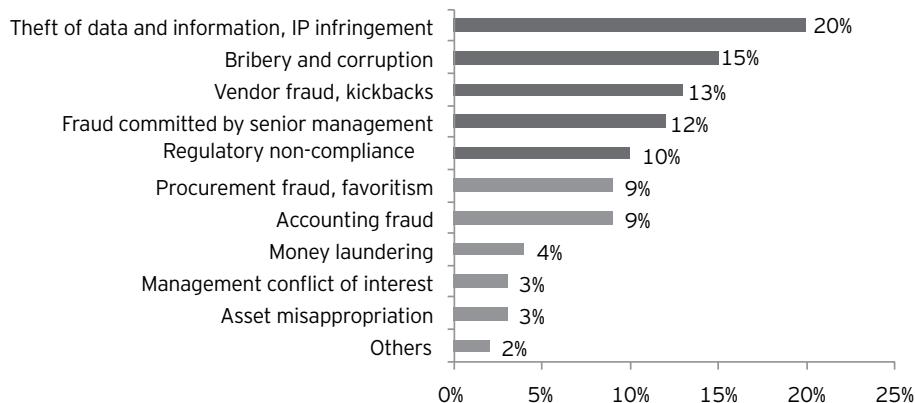
According to half of the survey respondents, the incidence of fraud has increased in their industry. In addition to industries such as banking, Non Banking Financial Companies (NBFC), real estate and telecommunications, which are generally perceived as being highly fraud prone, around 50% of the respondents from infrastructure, IT/ITeS and consumer product companies also indicated that fraud incidents have increased in their segments.

Discovery of fraud - methodical or accidental

Only 14% of the respondents attributed detection of fraud to automated surveillance systems. It seems counter-intuitive that we still detect most cases of fraud by being tipped off or by accident, even with advancement in technology and heightened regulatory activity. Therefore, now, more than ever, there is a need to apply advanced analytics to fraud detection.

Figure 1: Fraud risk

Q: Which of the following types of fraud do you believe can pose the biggest risk to your industry?



Cost of fraud - more than monetary

In the wake of recent scams and public activism against graft, there is a good chance that adverse news about a company may be blown out of proportion by the media. At such times, companies walk on a thin rope and are overtly conscious of potential fraud, as it may damage their reputation and market capitalization. In addition, they are also fearful of rating agency judgments on their risk management, which can influence availability and cost of capital.

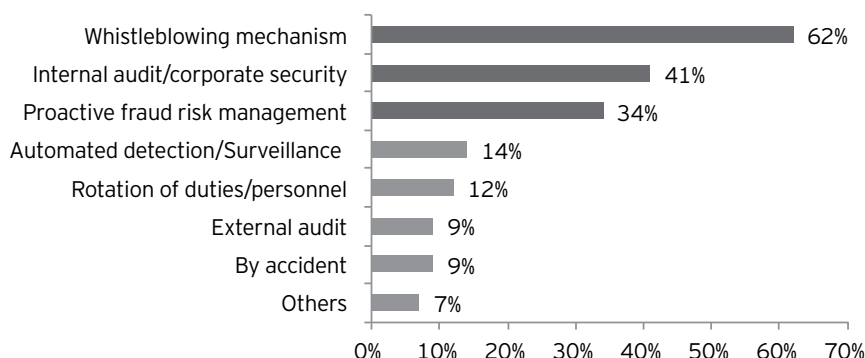
A respondent from the manufacturing sector said, "The root causes are increased use of technology, power without adequate checks, decentralization of operations, lack of internal checks and controls, falling moral values, disappointing character of national leaders, greed, etc."

For companies, public perception can have a dramatic impact on their business. According to more than three-fourth of the respondents, loss of reputation is the most serious collateral damage (actual or potential) stemming from fraud.

Around 80% of “enterprise data,” e.g., company documents, presentations, the internet, e-mail, etc., is unstructured, yet most of today’s automated, anti-fraud detection tools and audit techniques focus on 20% of structured data.

Figure 2: Methods employed to detect fraud⁷

Q: Has your company been subjected to any fraudulent incident during this last one year?
If so, which one of the following methods of detection were employed?



Current practices - inconsistent with globally accepted norms

Companies still using internal/statutory audit to detect fraud

Companies tend to over-rely on audits. Internal and external audit, and code of conduct seem to be the most preferred anti-fraud measures employed by companies. However, these methods are not sufficient for detecting fraud and limiting losses caused by it. There are only a few companies that have put in place proactive fraud risk management initiatives and have a whistle-blowing mechanism.

Corporate reluctance to seek legal recourse

Companies typically prefer to avoid reporting any economic offence to a regulator because of a

perceived threat to their reputation. They deal with such instances in a discreet manner by not letting even their employees know about such incidents, fearing that it would tempt others to attempt something similar. They are generally interested in recovering the defrauded money rather than getting the culprit punished under Indian laws, since it is not legally binding on them. Companies also hesitate to report such matters to the police, apprehending the hardships they may face during the investigation and prolonged judicial trials.

Corporate reluctance to seek legal recourse is a ground reality, and the reasons for this cannot be underestimated, but it is imperative to report the wrongdoing, so that the perpetrator is punished and the company can send out a strong message of zero tolerance for such misdemeanours to its employees and stakeholders.

⁷ Some percentages in this report total more than 100%, since executives can make multiple selections.

Only 35% of the respondents said that their companies take legal action against any employee responsible for committing fraud. Most companies do not take any disciplinary action against employees responsible for fraud.

Growing greed - profile of a fraudster

In the often-quoted fraud triangle of Donald R. Cressey, usually the motive for committing fraud is attributed to financial need, which a fraudster may be unable to meet with his or her regular income. However, in recent years, we have seen a change in the motive, as it shifts from "need" to "greed", with more and more people committing fraud to support their opulent lifestyles, which are not commensurate with their incomes. There are many real-life experiences and certain assumptions that form the basis for the traits of a fraudster, as drawn by the respondents in this study. These include the following:

- ▶ Young employees, especially in their 30s, who are at ease with technology, may commit fraud to make "quick money."
- ▶ Image projection in a sluggish economy and the prospect of accelerated career growth can motivate employees to bend rules for reasons beyond financial need.
- ▶ An employee working at an offsite location or in a remote satellite office, away from the direct control of management, has a greater opportunity to commit fraud.

- ▶ Sales and procurement are the two departments that have the maximum interaction with external parties. This offers employees working in these departments the opportunity of colluding with outsiders to exploit their insider and confidential knowledge about their companies, without coming in the direct line of suspicion.
- ▶ Lack of controls in rapidly growing organizations, where fraud may be overlooked as the cost of doing business, is another factor that can encourage fraud.

Given the high cost of occupational fraud, effective fraud-prevention measures are critical today. Fraudsters generally show behavioural warning signs of their misdeeds. These red flags, e.g., as living beyond their means or displaying control issues, cannot be identified by traditional control methods. Employees should be trained to recognize common behavioural signs that indicate that fraud is being committed and be encouraged not to ignore such red flags, since these may be the means of detecting or deterring fraud.⁸



Section 2:

Areas of concern



According to 15% of the respondents, management conflict of interest poses the highest fraud risk.

Data and information theft – managing insider threat

Till recently, India was the most sought after and preferred destination for companies looking to offshore their IT and back-office functions. However, some recent incidents of stolen data and fraud have raised concerns relating to privacy and data protection.

Some key risk prone areas:

- ▶ Increased vulnerability due to anytime and anywhere accessibility
- ▶ Leakage of company and customer's confidential information by current or ex-employees
- ▶ Loss of confidential data due to external vulnerability
- ▶ Manipulation of procurement, accounting or other IT-based process or system

Although insider threats are easy to understand, they are hard to detect as compared to external ones. Employee perpetrating fraud are generally allowed or authorized to access sensitive information or data to execute their routine jobs. To identify an individual who is misusing information is like looking for a needle in a haystack blindfolded. It is even more difficult than detecting the unauthorized access of an external hacker or intruder.

A respondent from the IT/ITeS industry said, "In the nature of our industry, fraud takes place more often due to false claims in employees' profiles with regard to their work experience, and also due to data violations such as unauthorized downloading of software, leading to serious intellectual property right violation issues."

According to a respondent, "Fraud occurs in any area and is not restricted to sales, and also not to middle or senior management, but is essentially perpetrated by people in position, who have the power to influence decisions and by those who are normally trusted."

Management's overriding controls

Public capital is the key driver of the growth of companies. Moreover, accessing markets is the preferred mode of raising capital in the case of many promoter-driven companies. However, this comes with strings attached, e.g., the expectation of and responsibility to shareholders and creditors, additional statutory compliance requirements and associated costs. The pressure on management to deliver results and manage expectations, irrespective of market conditions, is also very high.

A company usually has to walk the fine line between compliance and business efficiency, and erring on either carries a high penalty. Therefore, its management is expected to act as its guardian and implement suitable risk-based control structures to manage compliance and business requirements.

It has been observed that the tighter control a company has over its audit functions, the more likely it is that at some point this will become ineffective. In difficult market conditions, its management members may succumb to the pressure of "keeping up appearances" and ignore the controls they are meant to safeguard.

Supply chain leakage facilitating counterfeiting in consumer product industry

The consumer product supply chain is complex in nature, and the industry witnesses tough competition, which pushes companies to be highly cost-efficient. This necessitates that large FMCG companies primarily depend on third-party (3P) vendors for their supply of raw materials, packaging as well for contract manufacturing. High-growth pressures and aggressive expansion plans tend to make the management of such companies frequently overlook the importance of setting up proper controls over and monitoring mechanisms for their third-party vendors. The supply chain is especially vulnerable to leakages at the nodal point of third-party vendors, as compared to other nodes such as company- managed plants, warehouses, distribution centers and retail stores. What makes fraudulent incidences even more difficult to detect and to distinguish fake products from genuine ones is the fact that the material used by counterfeiters to manufacture spurious products often seems genuine. This is a problem that is clearly crying for redressal.

Counterfeiting leads to loss of revenue, attrition of customer satisfaction, damaged brand integrity, price distortions and the development of a gray market

for goods. Quite often, the original material is used to manufacture counterfeit products. Counterfeiters generally manage to infiltrate a company's supply chain and encompass third-party vendors, warehouses and 2P vendors that siphon off material. Once they have access to original material, it is easy for them to assemble counterfeit products with a minimal investment, e.g., in a cottage industry.

Probable leakage points in the supply chain:

- ▶ **Scrap channel:** Sometimes a stock of unused material is scrapped without it being destroyed. Material discarded in this manner can be easily used to assemble spurious products
- ▶ **A parallel supply chain:** Counterfeiters can infringe a company's original supply chain and source genuine material from it.
- ▶ **Improper disposal of obsolete and expired stock:** In some cases, companies fail to control disposal of their obsolete and expired stock, and counterfeiters obtain these products from the companies' managed units.
- ▶ **Leakage from company warehouses:** Finished products are stolen from the warehouses and plants of companies, and are sold at discounted rates.





Bribery and corruption - the perpetual challenge

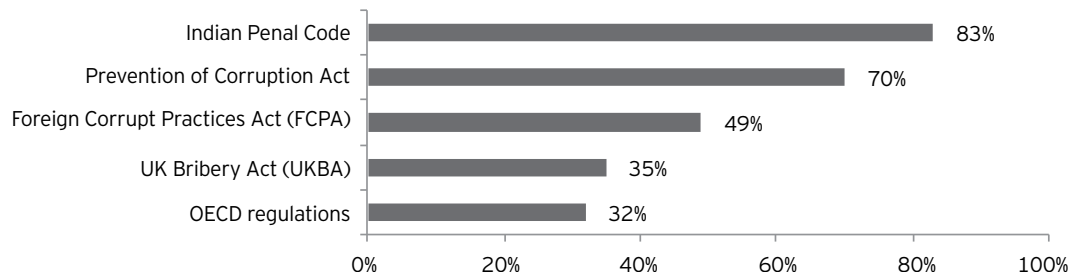
Bribery and corruption are undoubtedly the most frequently discussed topics in the business world today. The world has been witnessing multimillion dollar scams and India is not far behind. Bribery and corruption may be as old as mankind, but the key issue faced by India today is not petty bribery, but high-level corruption, which has had a significant impact on the country, its people and its image.

Increased awareness of local laws, but low awareness of global ones

After the recent scams, there seems to be an increased awareness of anti-graft laws, and nearly three-fourth of the respondents indicated that they were aware of anti-corruption legislation in India – the Prevention of Corruption Act. However, although three-fourth of the respondents represented MNCs, less than half of them were aware of important anti-graft legislation such as the US FCPA and the UK Bribery Act, both of which have extraterritorial reach.

Figure 3: Increased awareness of anti-corruption laws⁹

Q: Are you familiar with the following Acts or regulations?



A respondent from a multinational company, in response to a question on anti-graft legislations, said, "There is no level playing field for multinational companies in India. The enforcement environment is strict in MNCs (as compared to Indian companies) due to FCPA regulations. This is especially true of the interaction of such companies with government agencies, poses challenges for them and places them at a competitive disadvantage as compared to their Indian peers."

⁹ Some percentages in this report total more than 100%, since executives make multiple selections.

Cash seems to be the most popular mode of paying bribes. More than half of the respondents selected it from the long list of possible modes. In India, where it is the customary and accepted practice for people, even corporate organizations, to exchange gifts, 21% of the respondents selected this as the second most common mode of paying bribes.

Rationale for bribery

Nearly one-third of the respondents said that the practice of giving “kickbacks to win or retain business” is prevalent; one-fourth of respondents indicated that this practice was followed “to get routine approvals from government agencies” and “influence people in making favorable decisions.”

The responses given above are supported by the results of the Ease of Doing Business Index¹⁰ of the World Bank, in which India is ranked 132nd out of 183 economies. This highlights the various delays and difficulties faced by investors or companies in setting up businesses and attempting to obtain routine licenses and permits in the country.

Unfortunately, corruption is frequently perceived as the way of doing business in India, and many people believe it is an acceptable practice to expedite routine governmental action, e.g., obtaining approval, by employing corrupt means such as giving bribes. An investor or a company may be exposed to bribery and corruption risk at various stages of its setting up business, beginning from its corporate incorporation to its setting up a manufacturing facility, from importing raw materials to exporting finished products and from multi-location expansion to obtaining foreign funding. It is therefore essential for it to be cognizant of these risks.

The rationale for bribery varies across industries. We have received diverse responses for different industries, for instance, the majority of the respondents from the telecom sector indicated that bribery is often used to win business, whereas respondents from the consumer products sector reported that it is frequently used to obtain routine administrative approval. The most blatant reports of bribery and corruption were from the respondents of the real estate segment, with 100% of them saying that bribery was a real bottleneck in the path of procurement of routine administrative approval in the sector.

Some companies in India take the easy way out and adopt various strategies of paying bribes. Appointing third parties and paying them, without availing of their services, is the most common methodology for doing this.

However, in our experience, we have seen that some companies appoint compliance officers to deal with government and related matters. They strictly refuse to pay bribes and follow the difficult path. They also try to imbibe this culture in their employees, suppliers and intermediaries. Accordingly we believe that with the right anti-bribery framework (including policy, procedures and monitoring) it is possible to do business in India with limited exposure to FCPA, UK Bribery Act or any other local statute.

According to Transparency International, corrupt politicians and government officials in developing and transition economies receive bribes totaling between US\$20 billion and US\$40 billion every year, which is equivalent to between 20% and 40% of all official development assistance provided.¹¹

10 “Doing business in a more transparent world: economic profile of India,” World Bank and International Finance Corporation report, 2012.

11 “What lies beneath? The hidden costs of entering rapid-growth markets,” Ernst & Young Master CFO Series, 2011.



Factors facilitating bribery and corruption

A respondent from a Private Equity (PE) firm said, "Government-facing industries witness the highest incidence of corrupt practices."

Many industries in India have historically been dominated by government-owned entities, since the regulatory environment in India is wide enough to control many private companies or the companies directly or indirectly supply to state-owned entities. It is because of this that certain industries and companies in India face a high risk of bribery and corruption.

Figure 4: Factors facilitating bribery and corruption¹²

Q: Which of the following are the main factors facilitating corruption?



Nearly 40% of the respondents indicated that the inherent nature of the industries in which their companies operated was responsible for facilitating corruption; 34% respondents said that it was due to the "weak tone at the top."

¹² Some percentages in this report total to more than 100%, since executives can make multiple selections.

Around 62% of the respondents were in favor of stringent disciplinary procedures and 73% said that their companies should adopt a zero tolerance approach to bribery and corruption, e.g., by taking legal action against perpetrators of fraud.

Fight against bribery and corruption

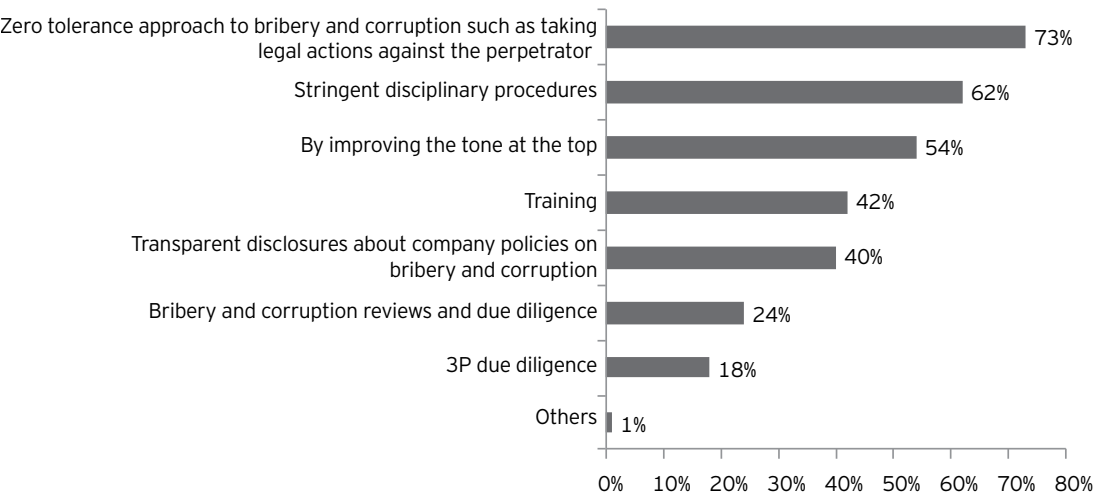
Companies can proactively take the first step against corruption by training their employees, implementing transparent policies and setting the tone at the top.

The good news is that a number of companies, irrespective of their country of domicile, are paying heed to the risk of bribery and corruption. The corporate world is changing and is proactively setting up an anti-bribery and corruption framework that is being increasingly implemented.

A respondent from a consumer products company said, “Corruption is widely prevalent in the country and the private sector is not totally immune to it. Strict compliance with the rule of law and ethics, setting of high internal standards and transparent behavior will help to reduce incidences of fraud.”¹¹

Figure 5: Steps to mitigate bribery and corruption risk¹³

Q: In your opinion, how can your industry fight bribery and corruption?



13 Some percentages in this report total more than 100%, since executives can make multiple selections.

Table 1:**From top to bottom: how management can embed a zero tolerance approach to bribery and corruption¹⁴**

These are several largely commonsense measures that will give employees a reason to care about complying with anti-bribery and anti-corruption regulations by effectively linking these with their work and career advancement. The leadership of an organization needs to incorporate the following in the company:

- ▶ Make ethical behavior a priority for the business and demonstrate its commitment to achieving this objective
 - ▶ Conduct a fraud, bribery and corruption risk assessment and identify any gaps in the company's current policies and procedures
 - ▶ Where necessary, implement changes in these procedures, paying particular attention to training
 - ▶ Ensure that training is tailor-made and relevant, reflects the issues and day-to-day problems employees are likely to encounter and guides them effectively on addressing them
 - ▶ Take a risk-focused approach to those who should be trained, on what, how and how often
 - ▶ Ensure that integrity is reflected in the company's appraisal system
-

14 "What lies beneath? The hidden costs of entering rapid-growth markets," Ernst & Young Master CFO Series, 2011.

Section 3:

Changing regulatory landscape



Table 2: Changing regulations in India

In recent times, several changes have been made in various laws and regulations relating to fraud, bribery and corruption, and others are being proposed. Some of these acts and proposed bills, with their changes and salient features, are summarized below:¹⁵

Bill/Law	Salient features
The Public Interest Disclosure (Protection of Informers) Bill, 2010 ¹⁶	<ul style="list-style-type: none"> ▶ Expected to encourage disclosure of information in public interest, but the private sector is excluded ▶ Provides limited protection to whistleblower ▶ Investigation not time bound
The Prevention of Bribery of Foreign Public Officials (FPO) and Officials of Public International Organisations (OPIO) Bill 2011 ¹⁷ (India's FCPA equivalent)	<ul style="list-style-type: none"> ▶ Criminalizes acceptance or solicitation of bribes by FPOs and OPIOs ▶ Criminalizes offers or promises to give bribes to FPOs and OPIOs for obtaining or retaining business
The Prevention of Corruption Amendment Act, 2011 (proposed amendment to the PCA, 1988)	<ul style="list-style-type: none"> ▶ Includes new sections that empower the Act to deal separately the offence of violating the norms of the Constitution, for using undue influence on public servants, misusing official powers and causing loss to the government exchequer ▶ Empowered to seize, attach and confiscate the property of convicted persons, who have amassed ill-gotten money
Companies Bill 2011 ¹⁸	<ul style="list-style-type: none"> ▶ Serious Fraud Investigation Office (SFIO): has powers to probe companies suspected of fraud ▶ SFIO's report filed in a court for framing charges to be equivalent to a police report under the Code of Criminal Procedure, 1973 ▶ To have the power to arrest persons for suspected fraud; SFIO to coordinate its operations with those of other investigating agencies such as the Central Bureau Of Investigation or Enforcement Directorate
Data privacy laws ¹⁹	<ul style="list-style-type: none"> ▶ To prevent use or gathering of personal information without the knowledge of the concerned persons ▶ To protect personal information, financial information such as bank accounts, credit or debit card or other payment instrument details
The Competition Act ²⁰	<ul style="list-style-type: none"> ▶ Anti-competitive agreements ▶ Abuse of dominant position. ▶ Regulation relating to combination

15 This information is intended to only provide a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice.

16 Bill No. 97 of 2010, The Public Interest Disclosure and Protection to persons making the Disclosures Bill, 2010; as introduced in the Lok Sabha on 26 August 2010.

17 Bill No. 26 of 2011, The Prevention of Bribery of Foreign Public Officials and Officials of Public International Organizations Bill, 2011.

18 Bill No. 121 of 2011, The Companies Bill, 2011.

19 "Ministry Of Communications and Information Technology", http://www.mit.gov.in/sites/upload_files/dit/files/GSR313E_10511%281%29.pdf, 11th April, 2011.

20 No.12 of 2003, The Competition Act, 2002; as amended by The Competition(Amendment) Act, 2007.

Section 5:

Tools for fighting fraud



An alarming number of respondents (61%) revealed that their companies rely on basic spreadsheet software for their IT fraud investigations.²²

Almost all companies, irrespective of their sector, are exposed to fraud, bribery and corruption risks, although the degree and complexity may vary.

Business leaders are aware of the need to address these risks, but lack of a comprehensive and integrated approach to fraud risk management continues to be a concern. Currently, companies' take the "check-the-box" approach to fraud risk management with isolated risk assessments, whereas the need of the hour is a cohesive but wider approach, aligned with their strategic business objectives.

The increasing number of frauds and the growing degree of risk necessitates that companies regularly review their policies, build in checks and use new and advanced technology to avoid such issues. Furthermore, although no system can be foolproof, a proactive and dynamic approach can make a company ready to counter fraudsters and gain an edge over its competitors.

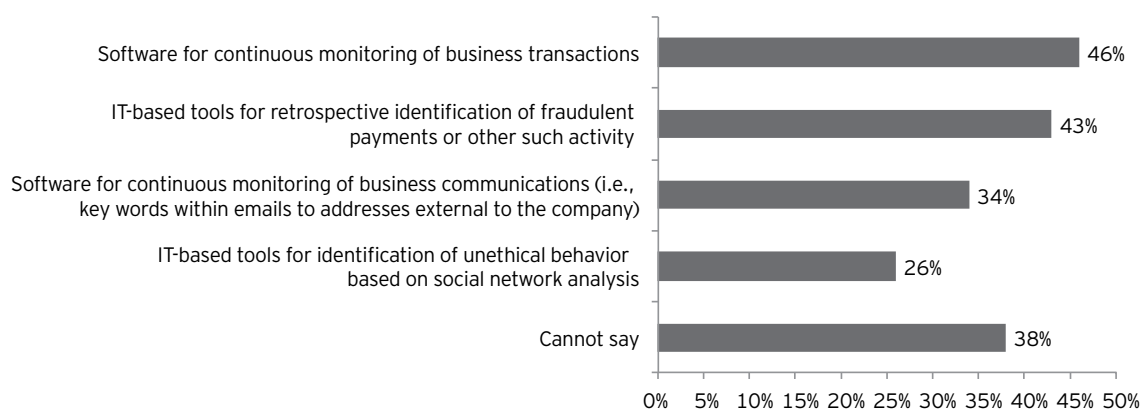
A respondent from the automotive sector said about fraud risk management, "Fraud cannot be completely avoided, but can be limited to a minimum with effective internal control, cross-functional teams to ensure verification, sound whistle-blower policies, commitment of top management and zero tolerance of fraud."

Role of technology

Less than 50% of the respondents are aware of fraud-prevention and detection tools. Moreover, in spite of the current popularity of social media, only one-fourth of the respondents were aware of IT-based tools that can be employed to identify unethical behavior, based on a social network analysis.

Figure 6: IT tools for fraud prevention or detection²¹

Q: Is your company familiar with any of the following fraud-prevention/detection tools?



21 Some percentages in this report total more than 100%, since executives can make multiple selections.

22 Technology fraud: a changing world, Ernst & Young, 2011.

One-third of the respondents were unaware of the IT Act 2000 and its amendments. We also observed minimal awareness of the Indian Evidence Act and the new data privacy law.²³

Some areas of their business in which entities can use technology to prevent and detect fraud:

- ▶ Using varied applications, with multitudes of databases in the background storing company data in a structured manner – such data being automatically and proactively analyzed to identify duplicate procurements, related parties doing business, ghost vendors, split purchase orders, inflated expense statements, etc.
- ▶ Restricting access to the function of copying and transferring data to prevent employees from gaining access to the company's and its customer's confidential and sensitive information
- ▶ Monitoring access to information to identify any deviation in pattern of usage that can help to identify at a later date "who accessed what and when"
- ▶ Classifying employee roles into "information roles," describing their need and right to access relevant information
- ▶ Text-based information, when analyzed rather than read, providing valuable insight into the "who, what and when" of fraud, especially since this relates to the third element of the fraud triangle – rationalization

Regulator's approach to technology

The banking sector is highly prone to fraud and leads all the other sectors when it comes to proactive fraud risk management. The possible reason for this is the active role played by the banking regulator, the Reserve Bank of India (RBI). A significant step taken by the regulator in 2009 was its issuance of the circular

on a fraud risk management system for banks; which made a bank's CEO, its audit committee and special committee accountable and responsible for the systemic failure of controls, or the absence of key controls or severe weaknesses in existing controls, which facilitated exceptionally large-value fraudulent incidences

In addition to the earlier guidelines given by the RBI, the regulator has recently released its report, "Working Group on information security, electronic banking, technology risk management and cyber fraud."²⁴

Some of the key recommendations of the Working Group include:

- ▶ A risk-based transaction-monitoring or surveillance process
- ▶ Quick fraud-detection capability to reduce losses and also serve as deterrent for fraudsters
- ▶ Banks to set up a transaction-monitoring unit within the fraud risk management group

A respondent from the banking sector said, "The vigilance committees in branches and administrative offices are merely ritual and need to be effective to conduct real-time monitoring."

With the help of forensic technology, a bank can turn risk management into a competitive advantage and also improve its business performance, but for this to become a reality, the commitment of its senior management is a prerequisite. Oversight from the top is essential for making the system effective.

²³ Technology fraud: a changing world, Ernst & Young, 2011.

²⁴ Working group on information security, electronic banking, technology risk management and cyber fraud report and recommendations, Reserve Bank of India, January 2011.

Whistle-blowing is at a nascent stage in India, and most Indian companies do not use it as an effective tool against fraud. Nearly a half of the respondents representing Indian companies revealed that their organizations do not have a whistle-blowing mechanism, while a large number of respondents (three out of every four) from Indian MNCs claimed to have one.

Whistle-blowing

Whistle-blowing is recommended under Clause 49 of the listing agreement²⁵ (SEBI's guidelines on corporate governance) and most Indian companies do not consider it necessary to implement it. They rely more on informal channels of communication, which they feel their employees will be comfortable using. Furthermore, they have apprehensions relating to misuse of the whistle-blowing mechanism for personal vendetta.

What makes whistle-blowing ineffective in Indian companies?

Most Indian companies that have a whistle-blowing policy use it as a "good to comply with" measure under Clause 49 recommendations. A look at the policies in practised by companies, however, reveals that their implementation of this policy can at best be described as rudimentary. The common features of the policy, which frequently render it ineffective, include:

- ▶ **Reporting employee faces risk of exposure:** In the absence of anonymity, employees are never comfortable about reporting fraud. They may be more at ease making a call than putting their names on a physical or digital document (email or website link).
- ▶ **Absence of a telephone (hotline) as reporting medium:** Less than half of the respondents reported that their companies have a telephone (hotline) for whistle-blowing. This is particularly important, given that global experience indicates that the majority of whistle-blowing tips are communicated through hotlines.
- ▶ **Operating hotline internally:** Around 90% of the respondents, who reported that their companies

had a whistle-blowing mechanism, revealed that these hotlines are operated internally. Given the fact that employees who decide to report a concern at the work place usually have to overcome an internal dilemma to report on their "colleagues," they may not be in a state of mind to write adequately comprehensive report, but are able to explain the concern when asked the right questions by a professional on the call. Furthermore, it is far more convenient to make a call and express a concern rather articulate it in writing.

- ▶ **Lack of awareness:** For effective implementation of a whistle-blowing mechanism, it is imperative to make employees aware about this medium for reporting fraud or misconduct. They should be sensitized to the fact that the mechanism is to be only used in exceptional cases when all other options of reporting have been exhausted. If an adequate awareness campaign is not rolled out, the mechanism tends to be misused for reasons that do not necessarily come under the purview of whistle-blowing. This may be the reason why 71% of the respondents said that only 10% of the complaints received through the mechanism require further investigation.
- ▶ **Process of categorizing and filtering complaints:** Another reason for the low number of complaints, which requires further investigation, is the probable absence of a process in organizations that can categorize and filter complaints. A meticulously drafted fraud response plan can help such organizations to opt for the correct action to be taken against complaints which are appropriately categorized and filtered. This also helps in weeding out "frivolous" complaints.

25 <http://www.sebi.gov.in/commreport/clause49.html>

According to 63% of the respondents, their companies have well-defined roles within their internal audit, compliance, risk and legal functions in the event of investigations, and 55% said that their companies had in place a clear procedure for reporting incidents, but only 32% have documented response plans.

Fraud response plan

Companies struggle to determine exactly who should be the people responsible for making a proactive and reactive response to reporting of fraud within their organizations, in order to ensure that they can prevent an inefficient response to such reports. The good news is that many companies now realize that such challenges need to be addressed. The bad news is that these very companies may not be able to overcome inconsistencies, duplicative efforts and a lack of communication within their companies because those responsible for anti-fraud efforts often operate independently of each other and not in a coordinated manner.

Fraud may still occur although the management has put in place the proper process, trained the company's employees on spotting problems, executed a robust fraud risk assessment initiative and designed internal controls to prevent and detect fraud. Therefore, it is essential for companies to formulate reactive elements for an effective anti-fraud program.

Well-documented and consistent fraud response plan

The cornerstone of a reactive element in an anti-fraud program is a competent team and its timely response to suspected fraud. It is essential to establish, review, approve and maintain policies and procedures relating to the company's response to fraudulent activities. Its fraud response plan should encompass investigations, remediation and uniform disciplinary processes. For an effective fraud response plan to work, it also has to communicate those who work on specific tasks from the moment an allegation is made till the point at which the results are reported.

To execute a fraud response plan effectively, it is necessary to establish an investigation protocol framework for a company's management. The protocols should state that all suspected fraud, regardless of the source, needs to be reviewed and investigated. A designated team should determine the person who will lead the investigation if external

assistance is needed, e.g., external forensic assistance with fraud, and the results of the investigation communicated to the audit committee in a timely manner.

Third-party due diligence

Third parties such as business associates, intermediaries, partners and vendors play a critical role in the success of a company. However, this association is tagged with a range of risks, the key among them being fraud, reputation and regulatory risks. Therefore, it is important that companies effectively assess the potential risk of conducting business with and develop appropriate risk management strategies in relation to third parties before engaging them.

While it is impossible to ensure that improper conduct will never occur, an appropriate level of due diligence can assist companies to proactively identify and manage risks arising from their association with third parties. Such due diligence can help them identify a wrong ethical "fit," legacy issues relating to fraud, regulatory non-compliance issues, unethical practises, misrepresentations, and questionable reputation and credentials.

Some of the risks that can be mitigated include:

Effective due diligence includes enquiries relating to business references and other customers helping a company understand the past track record of third parties in its commercial dealings.

Many government policies and an increase in law enforcement regulations have exerted increased pressure on companies to put in place appropriate third-party due diligence programs. Furthermore, in some recent regulatory developments, there has been a specific reference to third-party due diligence in Acts/policies/guidance on anti-corruption compliance programs. These include references to OECD's 2010 Good Practices Guidance on Internal Controls, Ethics and Compliance, the UK Bribery Act and the Federal Sentencing Guidelines.

Nearly two-third of the respondents said that their companies conduct due diligence on ethics and integrity for third parties. This positively reinforces the fact that globalization and the regulatory “push” is driving companies to proactively manage their fraud risk. Being more vigilant in managing third-party relations is another crucial step that needs to be taken in this direction.

However, the quantum of information that should be collected is dependent on several factors such as financial exposure, the criticality of the third party to a company's business, the nature of the activity to be performed, the extent of information already known, etc. Red flags resulting from such third-party due diligence can assist a company in developing appropriate risk management strategies, including its decision on whether it should associate with a specific third party.

Independent directors – a strong influence

In the past, it was common for directors to not specifically address fraud as a particular risk to their organizations. Also, there was no pressure on implementation of specific policies, procedures and controls for prevention and detection of fraud. However, the recent surge in incidences of fraud and the resultant confusion over the role of independent

directors has put this issue on the top of directors' corporate agendas.

In the last few months, we have seen independent directors taking a direct interest in reviewing the fraud risk management framework put in place by their organizations to mitigate the risk of fraud. With the introduction of new corporate governance requirements, which makes directors responsible for prevention and detection of fraud, directors have begun exercising adequate oversight on management of fraud risk worldwide. Non-compliance with these regulations or guidelines can have serious repercussions for all, including loss of reputation and personal liabilities.

While the management of a company is primarily responsible for implementing policies, procedures and controls for prevention and detection of fraud, those entrusted with governance, i.e., the Board of Directors or Audit Committee, have also been made responsible for prevention and detection of fraud.



About the research



Ernst & Young Pvt. Ltd. was assisted by a market research agency while conducting interviews. The survey was carried out online and in all we received 114 completed responses. The principal respondents included CXOs (42%), heads of internal audit, compliance and fraud prevention (14%), directors (9%) and mid/senior management (14%). A small minority (18%) report to these four main stakeholders. Respondents represented a sound mix of domestic companies and MNCs, with 45% foreign-based MNCs

and 32% represented Indian MNCs. The remaining 23% included Indian companies with domestic operations. The place of origin of the majority of foreign-based MNCs was the US (41%), followed by UK, Japan and Sweden (each 9%).

The respondents represented a wide range of industries and included the participation of banks and NBFCs, IT/ITeS and manufacturing companies, and Private Equity firms.

About Ernst & Young's Fraud Investigation & Dispute Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can distract you from your effort to achieve your company's potential. Better management of fraud risk and compliance exposure has become a critical business necessity for companies today, regardless of the industry sectors in which they operate. With our more than 1,400 fraud investigation and dispute professionals across the globe, we assemble the right multi-disciplinary and culturally aligned teams to work with our clients and their legal advisors, to give them the benefit of our broad sector experience, deep knowledge of relevant subjects and pertinent insights from our work worldwide. This is how Ernst & Young makes a difference.

- ▶ **Market intelligence:** We have dedicated field professionals, who are specifically experienced and trained in corporate intelligence, and are capable of conducting extensive market intelligence and background studies on various subjects, industries, companies and people.
- ▶ **Thought leadership:** We serve a variety of leading clients, which gives us a deep insight into a wide range of issues affecting our clients and business globally.
- ▶ **Qualified professionals:** We have a qualified and experienced mix of chartered accountants, certified fraud examiners, lawyers, CIAs, CISAs, engineers, MBAs and computer forensic professionals.

FIDS India

- ▶ **Deep competencies:** Our FIDS team has specific domain knowledge, along with wide industry experience.
- ▶ **Forensic technology:** We use sophisticated tools and established forensic techniques to provide the requisite services to address individual client challenges.
- ▶ **Global exposure:** Our team members have been trained on international engagements to obtain global exposure on fraud scenarios.

Our services

- ▶ Anti-fraud and fraud risk assessment
- ▶ Fraud investigation
- ▶ Dispute advisory services
- ▶ Forensic technology and discovery services
- ▶ Regulatory compliance
- ▶ Brand protection and IP risk
- ▶ Forensic business intelligence
- ▶ Anti-bribery program
- ▶ Third-party due diligence/Vendor due diligence

For more information please contact:

Arpinder Singh

Partner and National Director
Direct: + 91 22 6192 0160
Email: arpinder.singh@in.ey.com

Mukul Shrivastava

Executive Director
Direct: + 91 22 6192 2777
Email: mukul.shrivastava@in.ey.com

Anurag Kashyap

Director
Direct: + 91 22 6192 0373
Email: anurag.kashyap@in.ey.com

Sandeep Baldava

Partner
Direct: + 91 40 6736 2121
Email: sandeep.baldava@in.ey.com

Vivek Aggarwal

Executive Director
Direct: + 91 12 4464 4551
Email: vivek.aggarwal@in.ey.com

Jagdeep Singh

Director
Direct: + 91 20 6603 6119
Email: jagdeep.singh@in.ey.com

Ernst & Young Pvt. Ltd.
Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 152,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

Ernst & Young Pvt. Ltd. is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/india

Ernst & Young Pvt. Ltd. is a company registered under the Companies Act, 1956 having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

© 2012 Ernst & Young Pvt. Ltd. Published in India.
All Rights Reserved.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

EYIN1202-023

EY offices

Ahmedabad

2nd floor, Shivalik Ishaan
Near. C.N Vidhyalaya
Ambawadi,
Ahmedabad - 380 015
Tel: + 91 79 6608 3800
Fax: + 91 79 6608 3900

Bengaluru

12th & 13th floor
"U B City" Canberra Block
No.24, Vittal Mallya Road
Bangaluru - 560 001
Tel: + 91 80 4027 5000
+ 91 80 6727 5000
Fax: + 91 80 2210 6000 (12th floor)
Fax: + 91 80 2224 0695 (13th floor)

Chandigarh

1st Floor
SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: + 91 172 671 7800
Fax: + 91 172 671 7888

Chennai

Tidel Park,
6th & 7th Floor
A Block (Module
601,701-702)
No.4, Rajiv Gandhi Salai
Taramani
Chennai - 600 113
Tel: + 91 44 6654 8100
Fax: + 91 44 2254 0120

Hyderabad

Oval Office
18, iLabs Centre,
Hitech City, Madhapur,
Hyderabad - 500 081
Tel: + 91 40 6736 2000
Fax: + 91 40 6736 2200

Kochi

9th Floor "ABAD Nucleus"
NH-49, Maradu PO,
Kochi - 682 304
Tel: + 91 484 304 4000
Fax: + 91 484 270 5393

Kolkata

22, Camac Street
3rd Floor, Block C"
Kolkata - 700 016
Tel: + 91 33 6615 3400
Fax: + 91 33 2281 7750

Mumbai

6th Floor Express Towers
Nariman Point
Mumbai - 400 021
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 2000

14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (west)
Mumbai - 400 028
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 1000

5th Floor Block B-2,
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000
Fax: + 91 22 6192 3000

NCR

Golf View Corporate
Tower - B
Near DLF Golf Course,
Sector 42
Gurgaon - 122 002
Tel: + 91 124 464 4000
Fax: + 91 124 464 4050

6th floor, HT House
18-20 Kasturba Gandhi Marg
New Delhi - 110 001
Tel: + 91 11 4363 3000
Fax: + 91 11 4363 3200

4th & 5th Floor, Plot No 2B,
Tower 2, Sector 126,
Noida - 201 304
Gautam Budh Nagar, U.P. India
Tel: + 91 120 671 7000
Fax: + 91 120 671 7171

Pune

C-401, 4th floor
Panchshil Tech Park
Yerwada (Near Don
Bosco School)
Pune - 411 006
Tel: + 91 20 6603 6000
Fax: + 91 20 6601 5900