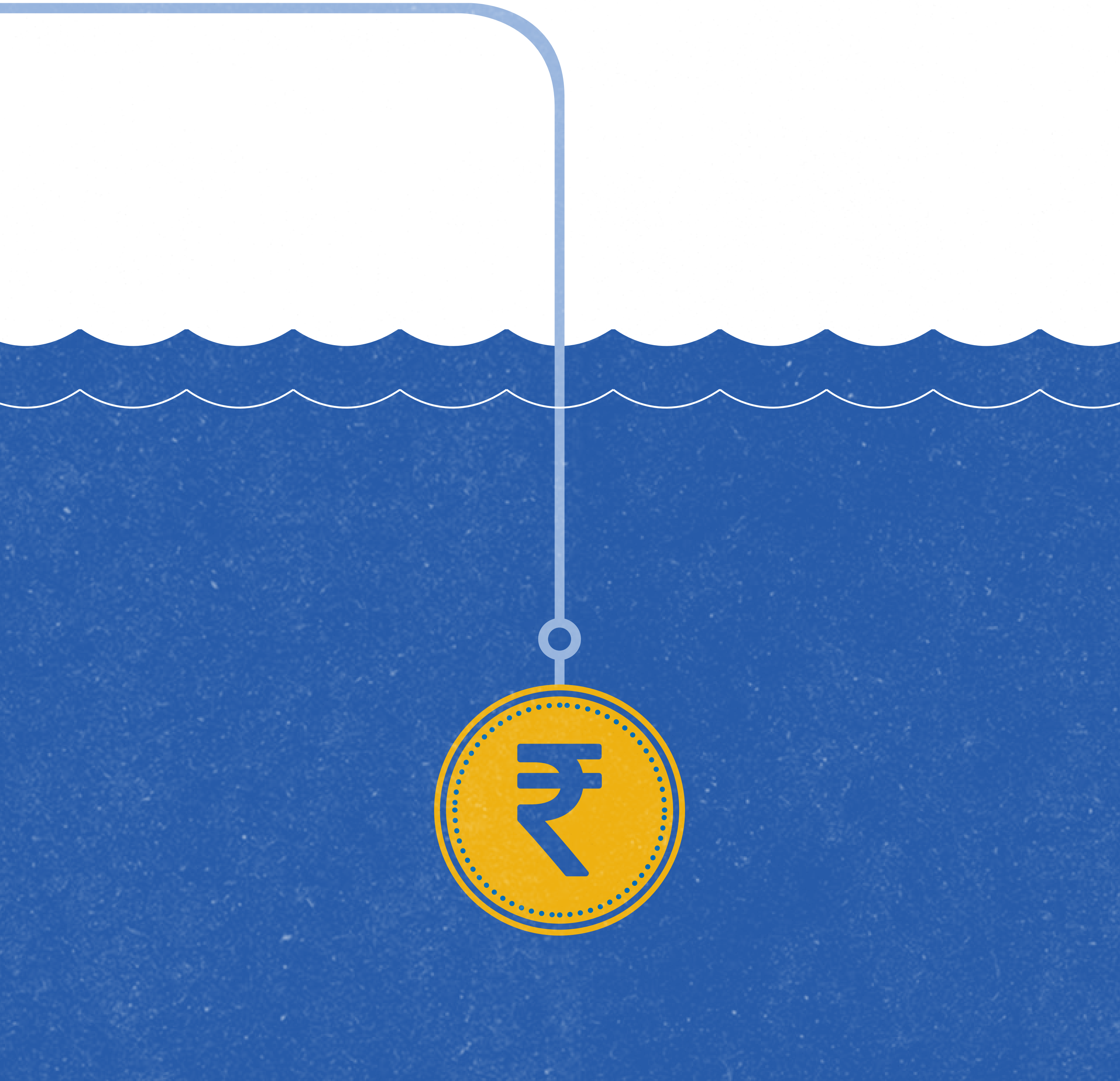
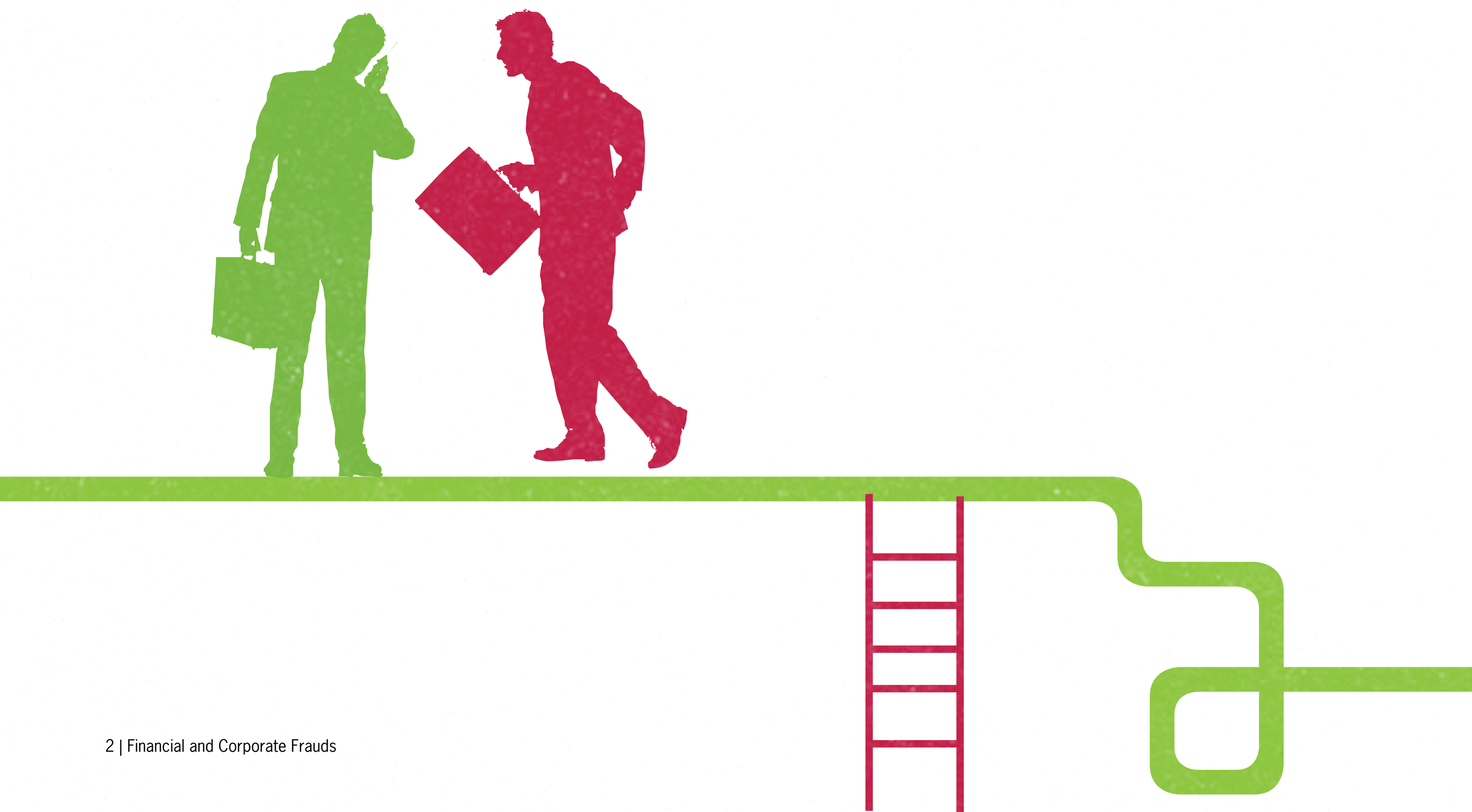
Financial and Corporate Frauds

July 2016, New Delhi





Foreword

Sunil Kanoria
President
ASSOCHAM

Financial frauds have emerged as an inevitable unwanted byproduct of economic growth. Taking advantage of the basic human attributes of aspiration and greed, fraudsters have duped millions across the world. They have also taken advantage of the lack of financial literacy amongst the masses. Global financial world is replete with such examples and India too has had its share of such scams. Investors had little ideal about a complex financial product such as Credit Default Swap (CDS) which triggered the global financial crisis in 2008. In India, people had very little idea about ponzi schemes; yet time and again people have lost their hard earned savings in a bid to make quick profits through such schemes. If the Enron episode resulted in huge value destruction, India had its own Satyam saga. Thus, financial frauds have emerged in all shapes and sizes throughout history.

In fact, things are becoming more challenging now. Devious ingenuity of the human brain is now leveraging technology to indulge in more sophisticated methods of crimes which are very much capable of creating systemic instability. Technology has overcome the barrier of distance and infiltrated almost every sphere of the networked life that we live today. A security threat today can be orchestrated by the click of a mouse. Phrases such as phishing, vishing, SMSishing, identity theft, data theft, online surveillance, digital espionage, ransomware, Dark Web, etc., which were beyond our imagination few years back, are now part and parcel of our lexicon. Technology has been a facilitator, but it can also be a disruptor if it is used by people with ulterior motives.

With India positioning itself as the world's fastest growing big economy and the country getting digitally connected both within and with the outside world, instances of financial fraud are bound to rise. It is t therefore imperative to prepare our country for coping with the emerging challenges. Our institutions should earmark budgets to make their systems fool-proof and train their people accordingly. Our regulatory bodies should be aware of what is happening on this front around the world and shape regulations accordingly. Financial literacy for the masses must figure on government's priority agenda.

I am very happy to note that ASSOCHAM is organising the 3rd National Conference on Financial & Corporate Frauds - "Risks, Challenges & Preventions". This knowledge paper prepared by Grant Thornton for this event tries to provide an overview on the trends on financial frauds, the role of technology in transforming frauds into systemic crisis, the changing regulatory landscape and the ways for fraud prevention and control. I hope the conference will delve in detail each of these aspects and come up with a set of workable solutions and recommendations on how to combat financial frauds and mitigate risks. I wish the conference a grand success.

Thank You,

Your Sincerely

Message

D.S. Rawat
Secretary General
ASSOCHAM

Fraud is as an intentional and deliberate act to deprive another person or institution of property or money by deception or other unfair means. Most of the financial frauds in the corporate fall under asset misappropriation and the submission of fraudulent statements such as concealment of liabilities, improper asset valuation, fictitious revenues, improper disclosures, etc. are some types of frauds. These practices cause severe damage to the financial system of institutions across countries. Similarly, with the help of leakages in systems of cyber and technology, fraudsters commit financial crimes. These damage the personal finance of individuals and the entire economy.

The growing capital infusion and increasing pace of business diversifications have a significant impact on the interest of all stakeholders. These associated interests are affected by the financial and corporate fraudulent practices. Despite the serious risk that fraud presents to businesses, many organisations still do not have formal systems and procedures in place to prevent, detect and respond to frauds. No system is complete fraud proof, but business can take steps to deter fraud and make it much less attractive to commit.

Corporate professionals such as accountants, auditors, risk controllers, finance heads etc., whose responsibility in the organisation calls for effective and efficient information and systems analysis, have a significant role to play in developing and implementing anti-fraud measures within their organisations.

ASSOCHAM is organising the 3rd National Conference on Financial and Corporate Frauds "Risks, Challenges & Preventions" on 1 July 2016 at New Delhi.

On this occasion the ASSOCHAM, along with Grant Thornton, as knowledge partner, has come up with a knowledge report to provide an advancement of knowhow on various anti-fraud resources, knowledge and tools along with the best course of action available to win over prospective frauds across organisations.

I am sure this knowledge paper will give rich insight and adequate knowledge to all stakeholders.

I wish the conference a great success.

With Best Wishes,

Foreword

Vidya Rajarao
Partner
Grant Thornton India LLP

Organisations of all types and sizes are subject to frauds. On a number of occasions, over the past few decades, companies have experienced financial reporting frauds, resulting in turmoil in the capital markets. In addition to this there is a loss of shareholder's value. In some cases, company also goes bankrupt. Therefore, it is imperative that organisations have a clear understanding of the threat that corporate and financial frauds pose. Organisations should also have the strategy to prevent such threats and the right controls and tools to mitigate such threats.

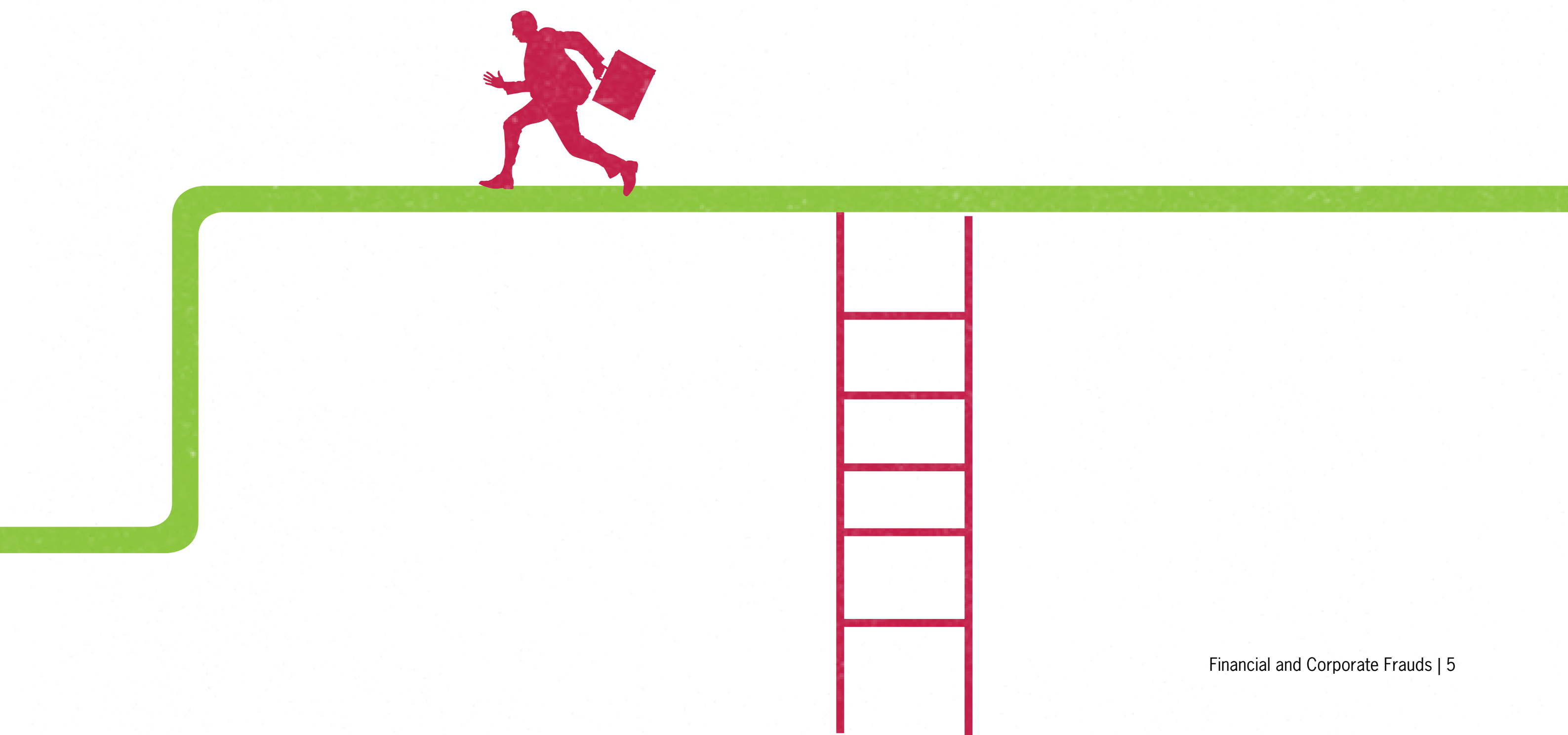
Further, continuous evolution of technology is changing the way in which organisations conduct business, sometimes creating opportunities for fraudsters to commit the crime. It is essential that organisations build processes, procedures and controls that do not needlessly put employees in a position to commit fraud and also effectively detect fraudulent activity if it occurs.

Finally, the responsibility of preventing, detecting and investigating corporate and financial frauds rests squarely on Board of Directors and this requires Board members to adopt preventive steps. Also, the Board of Directors and management should jointly agree and define their anti-fraud strategy, establish appropriate fraud mitigation steps and train their employees to combat financial and corporate frauds.

This paper provides an overview about financial and corporate fraud, and its consequences, risks faced by organisations, current challenges and the role and importance of preventive anti- fraud mechanisms.

We hope that these insights are helpful and we look forward to your feedback and comments.

With best wishes



Contents

1. Introduction

Indian market offers valuable opportunities for multinationals exploring inbound investments and local companies expanding overseas. Entering India either through a joint venture, acquisition or establishing a greenfield presence in India or consolidating and expanding current operations will be a critical component of growth for many international organisations. At the same time, understanding the risks in India is critical for the survival of business operations.

According to the Association of Certified Fraud Examiner's "Report to the Nations 2016" India ranks second in terms of victim organisations reporting the cases. The study shows the imperative need for regulators, business as well as the investment community to assess the risks emanating in the businesses. Today, in an increasingly interconnected world, digitisation enables businesses to be conducted in the wink of an eye. The digitisation also helps disguise the identities and machinations of people conducting that business, thereby enabling fraud to become more sophisticated and pervasive.

Thus, it is time for organisations to examine the role of corporate governance, particularly of those involved in preventing and detecting frauds.

2. Financial and corporate fraud: An overview

Corporate fraud can be classified in three broad areas:

1. **Financial fraud or Accounting fraud** consists of falsifying financial information by fudging the books thereby misleading the investors. The most popular accounting schemes are capitalising expenses, side deals, swap transactions, channel stuffing, accelerated revenues and deferred expenses. This is usually perpetuated by management.
2. **Self-dealing by corporate insiders** is mostly related to misappropriation of corporate assets by senior executives such as loans granted to senior management that are never intended to be repaid, failure to disclose forgive loans, reimbursed personnel expenses and extra ordinary personnel expenses charged to the company. Other such frauds are insider trading, misuse of corporate property for personal gain, kickbacks and individual tax violations related to self-dealing.
3. **Obstructive conduct** is falsifying testimony to regulators, erasing computer files, shredding documents, creating or altering document to support illegal conduct

Past incidents that highlight the extent of loss from financial fraud

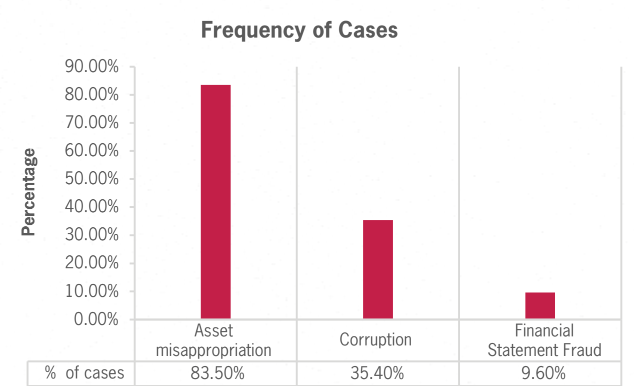
Some of the greatest accounting incidents of all time have rocked the financial and even political worlds with their repercussions. These have been felt across continents. A majority of these scandals are perpetrated on investors of the organisation in question. Investors were often misled and are forced to believe that organisation's financial situation is sound. However, this was not true.

S.No.	Organisation	Loss	Modus Operandi
1	Toshiba (2014)	Profits were overstated by more than US$ 1 bn	Toshiba understated its costs on long-term projects. Toshiba CEOs put intense pressure on subordinates to meet sales targets, which pushed certain employees to postpone losses or push forward sales on accounting
2	Olympus (2011)	US$1.7 bn accounting fraud- speculative investment losses	Olympus created a Tobashi scheme to shift losses off the Olympus balance sheet. Companies located in Cayman Islands were purchased via exorbitant M&A fees.
3	Satyam (2009)	Falsely boosted revenue by US$ 1.5 bn	Falsified revenues, margins and cash balance to the tune US$ 1.5 bn.
4	Lehman Brothers (2008)	Hid over US$ 50 bn in loans disguised as sales	Allegedly sold toxic assets to Cayman Island banks with the understanding that they would be bought back eventually. Created the impression Lehman had US$ 50 bn more cash and US$ 50 bn less in toxic assets than it really did.
5	Bernie Madoff (2008)	Tricked investors out of US$ 64.8 bn through the largest ponzi scheme in history	Investors were paid returns out of their own money or that of other investors rather than from profits
6	WorldCom (2002)	Inflated assets by as much as US$ 11 bn, leading to 30,000 lost jobs and US$ 180 bn in losses for investors	Inflated assets by as much as US$ 11 bn, leading to 30,000 lost jobs and US$ 180 bn in losses for investors
7	Enron (2001)	Shareholders lost US$ 74 bn, thousands of employees and investors lost their retirement accounts, and many employees lost their jobs	Kept huge debts off balance sheets

3. Threats to the organisations

Irrespective of the size and worth of any company and organisation, frauds occur regardless of their for-profit or non-profit status. Most of the smaller level frauds are never reported or discussed in the media or comes in the public eye. This is because of their size and very often because of the investigative design.

Frauds can be grouped in various categories. For example, from a legal perspective, frauds can be distinguished between: frauds by the organisation and frauds against the organisation. Frauds committed by the organisation carry legal risk, that is, potential civil, regulatory, and criminal liability. Frauds committed against the corporation carry financial risk, that is, the loss of income or assets. External and internal misappropriations of assets are by far the most common fraud against the organisation.



Source: Association of Certified Fraud Examiners (ACFE) report to the nations, 2016
The numbers include the frequency of the cases which fall under more than one category

Some of the key risks to the organisations are:

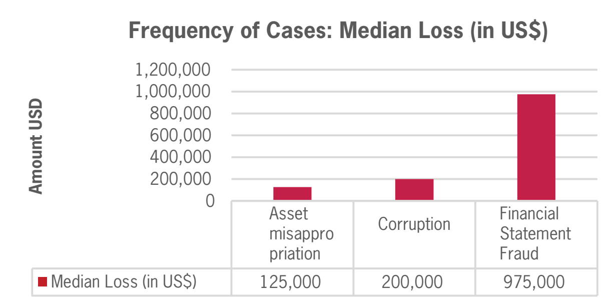
Fraudulent financial reporting:

Financial statement fraud is deliberate mis-representation, mis-statement or omission of financial statement data for the purpose of misleading the reader and creating a false impression of an organisation's financial strength.

Financial statement frauds include improper revenue recognition, manipulation of liabilities, manipulation of expenses, improper disclosures on financial statements and overstating assets, misuse of accounts, inappropriate journal vouchers, and suspense accounting fraud.

The finance and accounting function of any organisation can misuse their position within the organisation and manipulate the processes and bypass controls to derive personal gains or any other malafide motif.

A recent survey by Association of Certified Fraud Examiners (ACFE) indicates that although financial statement frauds were observed in 10 percent cases, there was a median loss of US $ 975,000.



Source: ACFE report to the nations, 2016

Related party transactions:

There are many types of related party transactions that might potentially be used to mis-state financial reports. The most frequent type of transactions that require regulatory action are concessionary loans to related parties, payments to company officers for services that were either unapproved or non-existent, transfer of funds through overvalued purchases of assets/investments, and sales of goods or services to related entities in which the existence of the relationship was not disclosed.

Generally, related party transactions are not necessary a mechanism for fraud. Their presence need not indicate fraudulent financial reporting. At first sight a related party transaction is represented to be of a benevolent/benign nature. An implication is that it is important for the auditor to understand the benign nature of most related party transactions, the differentiating features between benign and fraudulent transactions, and the importance of evaluating a company's related party transactions in light of its broader corporate governance structure.

Procurement fraud:

Procurement fraud can be of multiple types and is one of the most widely used modus operandi for siphoning off funds and window dressing the financial statements. Often defined as any illegal conduct through which the offender gains advantage, avoids an obligation or causes damage to an organisation. Procurement fraud can also be defined as the unlawful manipulation of the procurement process to acquire goods /services, obtain an unfair advantage, avoid an obligation or cause a loss to public property during the procurement process by public servants, contractors, or any other entity involved. Some of the methods to do so are:

- bid rigging/bid splitting;
- creation of shell companies to facilitate fraudulent payments;
- collusion between employee and suppliers;
- purchase order and contract variation orders;
- unjustified single source awards;
- false invoices for products and services for suppliers who do not exist

Payroll fraud:

Payroll fraud is the theft of cash from a business via the payroll processing system. There are several ways in which a payroll fraud can occur such as:

- advances not paid back
- buddy punching
- ghost employees
- pay check diversion
- pay rate alteration
- unauthorised hours

Tax evasion and money laundering:

Money laundering is a criminal offence aimed at presenting wealth of illicit origin or the portion of wealth that has been illegally acquired or concealed from the purview of tax and other authorities, as legitimate, through the use of methods that hide the identity of the ultimate beneficiary and the source of the ill-gotten profits.

False employment credentials

Falsified credentials are a growing concern for organisations, as job applicants fill their resumes with bogus academic degrees and job titles. The real risk comes when these applicants get the job and perhaps land in high-profile positions, as in the case of former Yahoo CEO Scott Thompson, whose four-month tenure ended after controversy over whether he had embellished his official bio.

Fraudulent expense claims

This is the easiest means of stealing some money from an organisation. Employees inflate their expense reimbursements and derive gains from the company.

Misappropriation of Assets:

Asset misappropriation schemes include both theft of company assets, such as cash or inventory, and the misuse of company assets, such as using a company car for a personal trip.

4. Challenges

With the increased prevalence of fraud and the negative consequences associated with it, there is a strong argument that companies should invest resources and time to tackle it. A joint Grant Thornton and ASSOCHAM survey conducted in 2015 revealed that cases of financial fraud have risen in India over the last few years and has become one of the main factors deterring foreign companies from investing in India. As the economy is growing increasing corporate frauds will prove to be disastrous for India. Some of the key challenges prevalent in the current environments are:

4.1.1 Challenges in detecting financial statement fraud

Detecting management fraud using normal audit procedures is a difficult task. There is a shortage of knowledge concerning the characteristics of management fraud. Financial managers and accountants at organisations who understand the limitations of an audit and standard auditing procedures are deliberately trying to deceive external auditors and investors by 'cooking the books'.

Further, there is a lack of mindset while evaluating the risks and recognises the possibility that a material mis-statement resulting from fraud could be present, regardless of any past experience with the entity. Consistent to this fact organisations sometimes not recognise the need to involve fraud specialists during audits because of cost considerations.

4.1.2 Inability to perform an effective fraud risk assessment

Organisations' focus on risk assessment usually tends to be more on general operational risks, regulatory risks and financial reporting risks, rather than fraud risks. This can make it difficult to view fraud in isolation and consider industry specific risks and potential fraud schemes as part of the fraud risk assessment.

4.1.3 Technology

Technology is a double-edged sword. As technology is advancing fraudsters are able to find ways to use it and perpetrate a fraud. Tech-savvy fraudsters are using technology in a variety of ways to commit frauds. Some include creation of false or misleading information in accounting records. Most accounting software systems allow users to have specific access to only certain aspects of the system. These include accounts receivable, account payable only. However, unauthorised access and password sharing is another area by which perpetrator have access on company's sensitive information. This is a potential threat to organisations. Putting restrictions on what your employees have access to will limit the potential of misappropriation of assets but if an employee has access to all aspects of an organisation the potential for fraud is significantly increased.

4.1.4 Lack of appropriate monitoring of third parties

Most organisations do not communicate their expectations of integrity and ethical values to third parties. Further, despite the frauds and risks posed by third party actions (such as kickbacks, bribery/ corruption etc.), there is limited monitoring of their activities. Contract clauses are often not stringently enforced and due diligence practices undertaken are not comprehensive.

4.1.5 Limited ability to demonstrate ethical behaviour or compliance with an ethics programme

Although organisations have established ethics programmes, they may not always evaluate the effectiveness or tangible impact created through such programmes. Also, the pressure to meet targets and actions of senior management may tacitly encourage employees to overpower/ violate the organisation's message on integrity and ethical values. Such instances fail to demonstrate compliance with the ethics programme.

4.1.6 Lack of segregation of duties

Failure to segregate duties appropriately across multiple systems/manual processes can inadvertently allow employees to commit fraud or conceal fraudulent activity. For example, there could be cases where password sharing (for gaining access to system/ financial transactions) amongst a group of people has diluted internal controls, leading to fraud.

source:1. http://www.assocham.org/newsdetail.php?id=4837

5. Changing regulatory environment

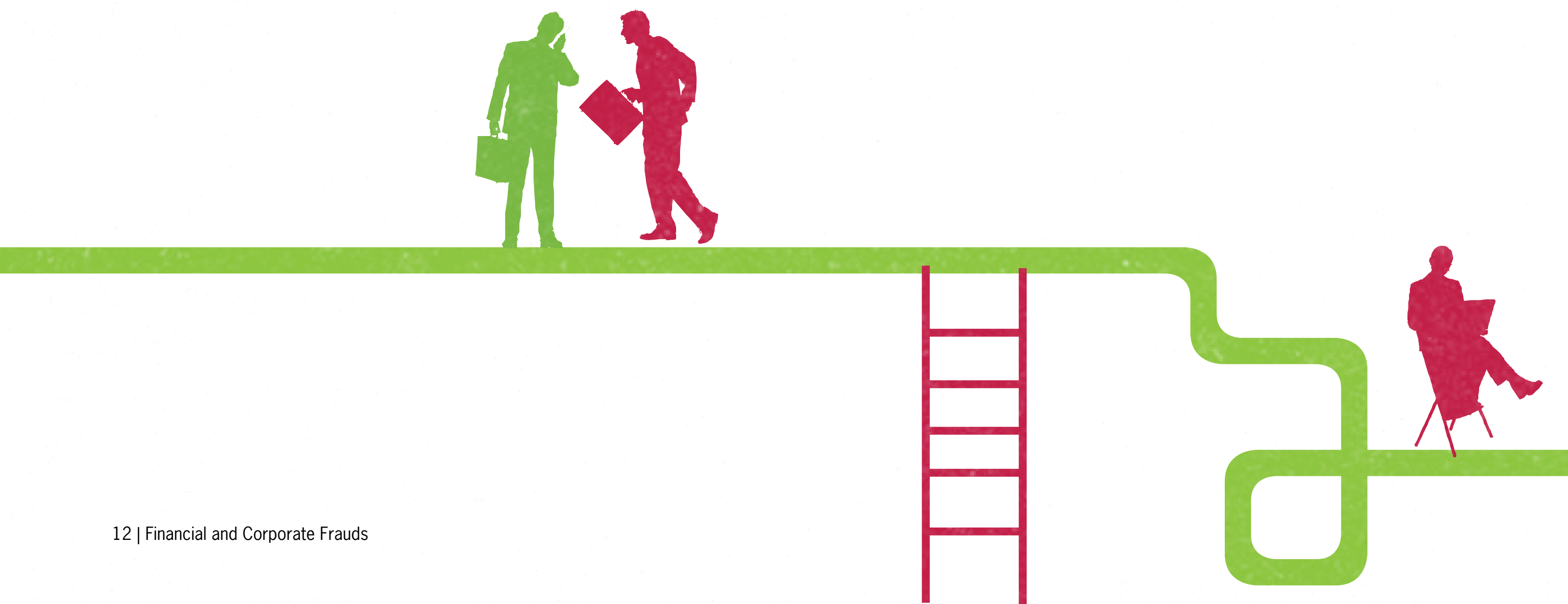
Some of the recent incidents have resulted in the increased focus of the regulators. Regulators are proposing companies to develop standards for fighting frauds and create framework to address fraud prevention, detection and response.

The new Companies Act 2013 is a step towards the evolution of India's regulatory environment. The Act includes specific provisions to address the risk of fraud, alongside prescribing greater responsibility and increased accountability for independent directors and auditors. It goes beyond professional liability for fraud and extends to personal liability, prescribing penalties for directors, key management personnel, auditors and employees.

The establishment of a vigil mechanism for listed companies, and a greater degree of accountability placed on the Board of Directors are the most effective provisions of the law.

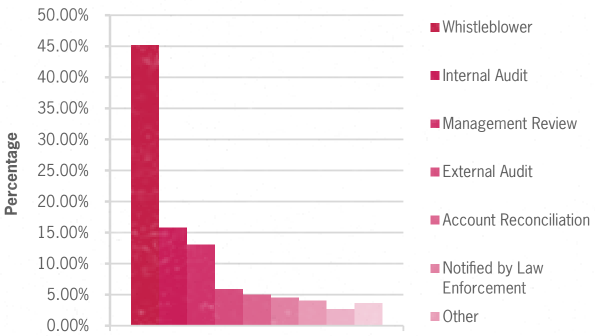
Several terms are used by globally recognised control frameworks and market regulators - Internal Control for Financial Reporting (ICFR) mostly in the US after the Sarbanes Oxley (SOX) Act and Internal Control (IC) mostly outside the US. The Companies Act 2013 (the Act) introduces a new term - Internal Financial Control (IFC) - which has certain features of IC and certain features of ICFR.

The Indian regulatory environment aspires to set up a legal framework to incorporate the global standards and provisions in its statutes. This convergence with the global laws is extremely important with the idea of bringing Indian corporate laws at par with the global standards and ensuring that the disparity in laws cannot be used to the advantage of fraudsters.



6. Prevention

Several financial frauds in the past and since the beginning of the century have repeatedly breached the trust of investors. Despite incidents of frauds, organisations still lack a formal system of fraud detection, prevention, and a response mechanism.



Source: We have provided here the analysis on the trends prevalent within South Asia, as per figures provided in the ACFE Report to the Nations 2016

Although, no system can give a 100 percent guarantee of prevention, the probability of their occurrence can be reduced to low numbers. The damages occurring on account of these frauds can be reduced by mitigating the risk factors associated with the businesses.

6.1 Formulating a strong anti-fraud programme:

A robust control environment is vital to reduce the risk on account of fraud and misconduct within companies and their dynamic business environment. The following are some key aspects of the anti-fraud framework that an organisation should implement to mitigate the fraud risks.

6.1.1 Leadership setting the tone:

Board of directors are responsible for setting the "tone at the top", which flows across the entire company and its various locations. Management views on mitigating fraud, corruption and misconduct should be revealed to the employees. It is recommended that management should actively assess frauds, corruption and misconduct risks and controls. Without ensuring that all suspected allegations of misconduct are independently investigated, management might not be able to develop the requisite neutral and balanced environment within the organisation. Disciplinary action and zero tolerance for violations should also be part of the message that the Board sends out to employees.

6.1.2 Fraud prevention policies:

Organisations willing to counter fraud should develop sound fraud prevention policies that must have the following key components:

- Extensive background checks on new-hires, promotion candidates, suppliers, customers and business partners (including international third parties);
- Segregation of duties;
- Position rotations;
- Limitations of physical access to assets; and
- Removal of unauthorised and old system users.
- Whistle blower mechanism

6.1.3 Ethics Code:

The ethics code of the company should be developed keeping in mind the size of the organisation, the mix of employees, the number of employees, and the key risk areas. Once developed, this code must be formally documented and communicated to the employees, third parties, and other stakeholders (official website of the organisation, if any). It should describe the disciplinary actions that can be initiated against people. This function should be continuously monitored.

6.1.4 Whistleblower or complaint mechanism:

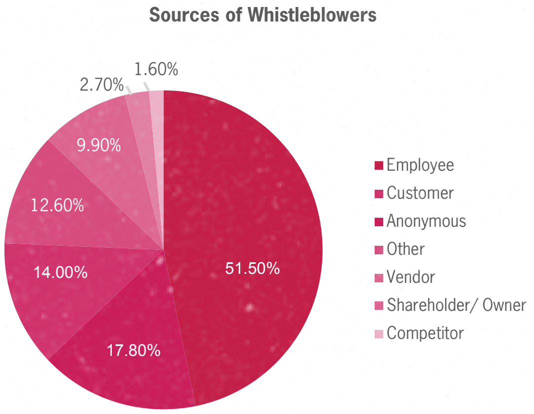
A whistleblower is a person(s) who has and reports insider knowledge of illegal activities occurring in an organisation. Whistleblowers can be employees, suppliers, contractors, clients or any individual who becomes aware of illegal or fraudulent activities taking place in a business either through witnessing the behaviour or being told about it.

The organisations need to consider the following:

- Maintaining anonymity of the complaint mechanism
- Ensuring confidentiality of information reported through the whistle-blower mechanism
- Policy of non-retaliation against the whistle-blower
- Actions that can be initiated based on the nature and seriousness of the issue reported?
- Issues that are "not serious" taking up senior executives' time.

- Concern about potential misuse of the channel, driven by personal agendas.
- Concern about compliance of policies or procedures with laws and regulatory guidance and global best practices.
- Concern about effectiveness of the mechanism.
- What more can be done using the mechanism.

As previously stated, whistleblowers are the most common source of detection for frauds. However, it is helpful and crucial to understand who is most likely to report fraud to the organisations. Below is the pictorial representation of the study carried out by ACFE across nations in 2016. This depicts the types of whistleblowers.



6.1.5 Training/awareness programmes to employees:

After policies and procedures are developed they must be effectively communicated and employees must be periodically trained. Some of the aspects to consider include:

- Management involvement in delivering the message
- In-person and web-based training
- Positive affirmation of policies
- Periodic reminders – once is not enough
- Consider annual confirmation for high risk functions
- Training people to recognise and report red flags to frauds
- Special training for finance professionals
- Special training for senior executives
- Special training for others in high-risk positions (i.e. business developers, sales and marketing)
- Broad roll-out of anti-corruption measures

6.2 Enhanced focus on identifying fraud risks:

The purpose of fraud risk assessments can be established with the below;

- Assessing the types of frauds that can impact business and identifying relevant types of fraud, such as fraudulent financial reporting, possible loss of assets, and corruption methods through which fraud and misconduct can be done
- Developing scenarios and considering the ways that frauds can occur, including management's stand (e.g., in the selection of accounting principles), susceptibility to management overriding and inculcating potential methods to circumvent existing control activities
- Understanding frauds through business partners and assess the manner in which work is performed by vendors, outsourced agencies and other third parties doing business for and on behalf of the company.
- Identifying and evaluate frauds and risks that bring change in the operating environment
- Identifying where the company should focus its anti-fraud resources and periodically review the results of the fraud risk assessment with the audit committee. Such periodic assessment should be helpful in challenging certain key aspects such as management override of controls
- Identifying areas of improvement

6.3 Continuous monitoring using data analytics:

Business data is increasingly being managed and stored by IT systems. The pressure to improve efficiencies and integrate supply chains has meant that many organisations are now heavily reliant on IT systems to support business processes. Such systems have also reduced the level of human intervention required, which has traditionally acted as a fraud control. As a result, organisations are placing more reliance on automated controls to both prevent and detect fraud.

The key aspects steps that organisations can consider to start are the following:

- Proactively monitoring key processes and run data analytics modules on internal/external communication, payroll and reimbursements, receivables and collections, sales and distribution, time and physical access controls and vendor payments.
- Develop a robust log maintenance policy and retention period of logs in line with fraud risk management requirements
- Develop notifications/alarms by which senior management can receive automated messages in case of process overrides
- Adequate control on devices containing confidential data, encrypt devices and use reliable software tools with remote data wiping capabilities to safeguard against device theft or intrusions

6.4 Due diligence on third parties:

Organisations mostly use services of third parties to manage their business operations and other activities. Sometimes working with third parties can significantly increase the risk of frauds. Organisations are able to extend limited control over their third party ecosystems and unlike some of the other countries, incorporating right to audit clauses in vendor contracts may be perceived as a breach of trust, damaging the business relationship. In these circumstances due diligence can be a useful tool to understand one's vendors and business partners.

These areas mentioned here can be covered by due diligence on third parties in order to address related fraud risks:

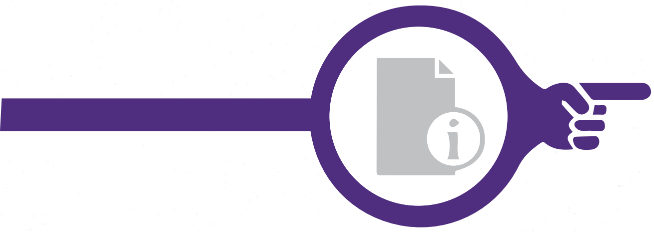
- Knowledge of third party background information, including ultimate beneficial ownership and affiliates, experience and competence/track record, any information on these fronts/shell companies for money laundering etc.
- Business interests/ affiliations, conflict of interest
- Any adverse news in media about unethical business practices, involvement in tax evasion, money laundering , terrorist financing or any bribery/corruption incidents
- Any Involvement in legal proceedings/ convictions for malpractice/crime etc.
- Any political affiliations, Inappropriate political support and links to politically exposed persons/entities
- Credit defaults and bankruptcies
- Other reputational concerns

7. Conclusion

Organisations are facing a number of challenges in the current economic scenario. They constantly deal with pressure of uncertain markets, escalating input costs, high labour turnover and advent of technology. Additionally, companies have to meet rising consumer demand across product categories with price innovation. Such challenges place further pressure on companies and their business partners. Such pressures may provide opportunity and incentives for fraudsters to commit frauds.

That past decade has witnessed a steep rise in the organisations which have increased the risk of fraud exposure. With any change in the environment of the businesses, the need to adapt to these changes is a prerequisite to attain sustainable growth. The change in the current environment is the increased fraud exposure for organisations. The response to this change is to equip our businesses against fraud risks and exposure through a systematic programme of fraud risk assessment, monitoring, incident response and remediation

8. Reference



Independent Studies:

- Association of Certified Fraud Examiner's "Report to the Nations 2016" http://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf
- Joint survey by Grant Thornton and ASSOCHAM http://www.assocham.org/newsdetail.php?id=4837

Articles:

Background Paper on Financial System Abuse, Financial Crime and Money Laundering— Prepared by the Monetary and Exchange Affairs and Policy Development and Review Departments.

Books:

- Corporate fraud: CIMA Publications, United Kingdom, www.cimaglobal.com
- Financial statement Fraud: Prevention and Detection by Zabihollah Rezaee and Richard Riley

About ASSOCHAM

The knowledge architect of corporate India, the Associated Chambers of Commerce and Industry of India (ASSOCHAM) is a premier apex chamber that has a membership of over 4 lakh companies and professionals across the country. It is one of the oldest chambers of commerce which started in 1920. It is also known as the "knowledge chamber" for its ability to gather and disseminate knowledge. Its vision is to empower industry with knowledge so that they become strong and powerful global competitors with world class management, technology and quality standards.

ASSOCHAM is also a "pillar of democracy" as it reflects diverse views and sometimes opposing ideas in industry group. This important facet puts us ahead of countries such as China and will strengthen our foundations of a democratic debate and better solution for the future. ASSOCHAM is also the "voice of industry" – it reflects the "pain" of industry as well as its "success" to the government. The chamber is a "change agent" that helps to create the environment for positive and constructive policy changes and solutions by the government for the progress of India.

As an apex industry body, ASSOCHAM represents the interests of industry and trade, interfaces with Government on policy issues and interacts with counterpart international organisations to promote bilateral economic issues. ASSOCHAM is represented on all national and local bodies and is, thus, able to pro-actively convey industry viewpoints, as also communicate and debate issues relating to public-private partnerships for economic development.

The road is long. It has many hills and valleys – yet the vision before us of a new resurgent India is strong and powerful. The light of knowledge and banishment of ignorance and poverty beckons us calling each member of the chamber to serve the nation and make a difference.

ASSOCHAM Offices:

The Associated Chambers of Commerce and Industry of India (ASSOCHAM)
5 Sardar Patel Marg, Chankyapuri, New Delhi – 110021
Tel: +91-11-46550555 Fax: +91-11-23017008/9 Website: www.assocham.org

Southern Regional Office	ASSOCHAM Western Regional Office
D-13, D-14, D Block, Brigade MM, 1st Floor, 7th Block, Jayanagar, K R Road, Bangalore – 560070 Telephone: +91-80-40943251-53 Fax : +91-80-41256629 E-mail: events.south@assocham.com, events@assocham.com, director.south@assocham.com	4th Floor, Heritage Tower, Bh. Visnagar Bank, Ashram Road, Usmanpura, Ahmedabad-380 014 Tel: + 91-79- 2754 1728 / 29, 2754 1867 Fax: + 91-79-30006352 Email: assocham.ahd1@assocham.com assocham.ahd2@assocham.com
Eastern Regional Office	**ASSOCHAM Regional Office Ranchi**
F 4, "Maurya Centre" 48, Gariahat Road Kolkata-700019 Telephone: 91-33-4005 3845/41 Fax: +91-33-4000 1149 E-mail: kolkata@assocham.com	503/D, Mandir Marg-C Ashok Nagar Ranchi-834 002 Email: Head.RORanchi@assocham.com Phone: +91-9835040255

About Grant Thornton India LLP

Grant Thornton in India is one of the largest assurance, tax, and advisory firms in India. With over 3,000 professional staff across 13 offices, the firm provides robust compliance services and growth navigation solutions on complex business and financial matters through focused practice groups. The firm has extensive experience across a range of industries, market segments, and geographical corridors. It is on a fast-track to becoming the best growth advisor to dynamic Indian businesses with global ambitions. With shorter decision-making chains, more senior personnel involvement, and empowered client service teams, the firm is able to operate in a coordinated way and respond with agility.

Over the years, Grant Thornton in India has developed a host of specialist services such as Corporate Finance, Governance, Risk & Operations, and Forensic & Investigation. The firm's strong Subject Matter Expertise (SME) focus not only enhances the reach but also helps deliver bespoke solutions tailored to the needs of its clients.

Contact us

To know more, please visit **www.grantthornton.in** or contact any of our offices as mentioned below:

NEW DELHI
National Office
Outer Circle
L 41 Connaught Circus
New Delhi 110001
T +91 11 4278 7070

AHMEDABAD
BSQUARE Managed Offices
7th Floor, Shree Krishna Centre
Nr. Mithakali Six Roads
Navrangpura
Ahmedabad 380009
T +91 76000 01620

BENGALURU
5th Floor, 65/2, Block A,
Bagmane Tridib, Bagmane Tech Park,
C V Raman Nagar,
Bengaluru - 560093
T +91 80 4243 0700

CHANDIGARH
B-406A, 4th Floor
L&T Elante Office Building
Industrial Area Phase I
Chandigarh 160002
T +91 172 4338 000

CHENNAI
Arihant Nitco Park,
6th Floor, No. 90,
Dr. Radhakrishnan Salai
Mylapore
Chennai 600004
T +91 44 4294 0000

GURGAON
21st Floor, DLF Square
Jacaranda Marg
DLF Phase II
Gurgaon 122002
T +91 124 462 8000

HYDERABAD
7th Floor, Block III
White House
Kundan Bagh, Begumpet
Hyderabad 500016
T +91 40 6630 8200

KOCHI
7th Floor, Modayil Centre point
Warriam road junction
M. G. Road
Kochi 682016
T +91 484 406 4541

KOLKATA
10C Hungerford Street
5th Floor
Kolkata 700017
T +91 33 4050 8000

MUMBAI
16th Floor, Tower II
Indiabulls Finance Centre
SB Marg, Elphinstone (W)
Mumbai 400013
T +91 22 6626 2600

MUMBAI
9th Floor, Classic Pentagon
Nr Bisleri factory, Western Express Highway
Andheri (E)
Mumbai 400099
T +91 22 6176 7800

NOIDA
Plot No. 19A, 7th Floor
Sector – 16A
Noida 201301
T +91 120 7109 001

PUNE
401 Century Arcade
Narangi Baug Road
Off Boat Club Road
Pune 411001
T +91 20 4105 7000

For more information or for any queries, write to us at **contact@in.gt.com**

Follow us **@GrantThorntonIN**

GrantThornton
An instinct for growth™