Ever increasing fraud risks in the IT and ITeS sector
Over the past decade, the Indian IT-ITeS sector has grown rapidly and achieved significant milestones in terms of revenue, employment generation and value creation. In the given scenario, the omnipresent threat of frauds grew even faster than anticipated. New risks emerged as the severity, volatility and pace of change fostered opportunities and incentives for fraud.

The volatile economic situation over the past two years has aggravated the scenario, resulting in a steep increase in the value and quantum of frauds in IT-ITeS sector.

Some recent instances of fraud in the IT-ITeS sector:

**Employee embezzlement fraud:** An employee of a large software services company in India was able to steal the password of the bank account of the company and embezzle an amount in excess of US$4 million.

**Intellectual property infringement fraud:** An employee of a software development company in India sold off the source code of the new software developed by the company to its competitors.

**Forex fraud:** An employee of a leading software company in India without proper authorization hedged the foreign exchange receivable by the company outside the normal course of the company’s hedging process, which resulted in a loss of US$20 million to the company.

**Data theft:** An employee of a Gurgaon (India)-based BPO company is believed to have sold a CD, which is suspected to contain some confidential data pertaining to the customers of a British bank.

**Refund fraud:** Two employees working in a Chennai (India)-based BPO misused their authority and created 30 dummy customer e-mail IDs and embezzled more than US$91,000, which was supposed to be paid as refund for dissatisfied customers.

**Procurement fraud:** Two employees of a Bangalore-based technology company were sacked for allegedly showing preference to certain vendors/service providers and demanding favors from certain other vendors in lieu of the timely processing of their invoices/bills and the renewal of contracts.

**Recruitment fraud:** The entire recruitment team at the Indian subsidiary of a large IT company was sacked for allegedly accepting bribes from prospective employees and recruitment consultants.

**Payroll fraud:** An employee of a Hyderabad-based company drew salary even after six months of leaving the company.

**Misappropriation of funds:** Few employees from the Pune center of a large Indian BPO opened several dummy accounts to transfer the customer funds to these fictitious accounts.

---

**Introduction**

“More than the exceptional results and ever-increasing customer base of the companies in the IT & ITeS sector, we have heard extensively about frauds being uncovered.”

Organizations’ alert! It could happen to you!
The key reasons why such incidents of employee frauds have taken place:

The absence of policies and procedures aimed at preventing and deterring employees/vendors from committing fraud contributes immensely to rising fraud cases. In some organizations while the policies exist, the same may not have been communicated adequately and appropriately.

Another key reason is the high growth rate in the information technology sector, coupled with an even higher attrition rate. This lethal combination puts extreme pressure on processes/controls and could lead to non-adherence to established processes and controls, which ultimately results in financial/efficiency/reputation loss.

There are inadequate infrastructure/processes for performing employee background checks. Currently, NASSCOM has worked to set up a national database of employees working in the IT and BPO sector in India known as the “National skills registry.” However, the validation and registration of the IT and BPO employees require authorization from the employees themselves.

The misuse of the trust and responsibility obtained in an organization is another key cause for committing frauds. In several cases investigated by us over the last five years, we have seen that senior/middle management employees, who have obtained a higher level of trust and responsibility within a company, are more likely to commit fraud by misusing the authority and trust bestowed on them.

The pressure of expectations has been a determining factor for some of the employees in their attitude towards fraud.
Impact of fraud

- Fraud incidents cause severe damage to the reputation of the company.
- In many cases, fraud instances have resulted in direct loss of business to the company.
- Fraud incidents may expose the company to civil or criminal liabilities.
- Legislative requirements or compliance procedures are bound to increase in the light of fraud cases.

Legislative requirements regarding fraud risk management:

- To address the issue of data protection, the government had introduced the Personal Data Protection Bill in 2006. However, it did not come into force till date. The issue of data protection is to a certain extent addressed by the introduction of the Information Technology (Amendment) Act, 2008. However, it does not cover the issues of data protection for data sent outside the territories of India.
- Legislations such as The Sarbanes Oxley Act, The Foreign Corrupt Practices Act & SAS 99 require the management of US/US-listed companies to set up strong internal controls for the prevention and detection of fraud.
- Similarly, Indian legislations such as Clause 49 of the Listing Agreement and the ‘Standards on Auditing 240’ has put the primary onus for the prevention and detection of fraud on the management and those charged with governance.
- In accordance with the “Corporate Governance Voluntary Guidelines 2009” released by the Ministry of Corporate Affairs: “Companies should ensure the institution of mechanism for employees to report concerns about the unethical behaviour actual or suspected fraud, or violation of the company’s code of conduct or ethics policy.”

Most customers and regulators understand that possibility of such fraud instances does exist. However, they consider the following mitigating factors:

- What preventive mechanism does an organization have in order to prevent such fraudulent acts?
- How quickly and how well can the organization respond when such instances of fraud actually happen?

In the best interest of the IT-IteS companies, they need to proactively undertake a self-assessment of their existing fraud prevention processes and controls. IT-IteS companies need to ensure that the existing processes and controls are robust and are operating effectively to prevent the occurrence or recurrence of such incidents.

Fraud is too costly to leave it without proper attention.

“The recent cases of fraud have raised questions over the preparedness of organizations in preventing, detecting and handling frauds.”
The watch word is “Always Prevention!”

The likelihood of fraud can be reduced by implementing antifraud programs and controls. Besides the development of comprehensive policies and procedures, implementation of antifraud programs requires effective communication, implementation and compliance monitoring. This can be achieved in three steps as described below:

1. Create an anti-fraud environment

Management should strive hard to create an environment where people believe that fraudulent acts will not be tolerated at all, i.e., a zero tolerance level should be established for fraud/other dishonest acts. This can be achieved through the development and implementation of:

- **Fraud policy:**
  The development and communication of a strict fraud policy is expected to set the standard for intolerance of fraudulent behavior. This policy should communicate that the company is committed and willing to take a proactive approach to prevent, detect and report fraud. Further, it should clearly state the consequences of fraudulent acts when fraud is uncovered.

- **Code of business conduct/ethics policy:**
  The code of conduct/ethics policy should be comprehensive and should describe acts that constitute unethical/non-acceptable behavior. Depending on the nature of operations, complexity and its size, an organization may devise a policy that is applicable to all the employees (and all operating units). Additional specific policies may be devised for specific operating units/certain categories of the management/key employees.

- **Whistle blower policy/fraud hotlines:**
  As multiple global surveys carried out by various organizations over the past several years have pointed out, fraud hotlines/tip offs are one of the most successful tools to detect fraud. An effective whistle blowing policy should be such that employees are able to report/voice their suspicions of fraud occurrence without the fear of disciplinary action or retaliation against them.
• Fraud response plan
The fraud response plan is a step-by-step process of the procedures that should be followed by management, should an incident of fraud occur. Too often, when an organization experiences an incident of fraud, the management is not aware of action to be taken, which exposes the organization to various vulnerabilities, including litigation.

• Fraud awareness training sessions and workshops
A crucial element in preventing fraud in organizations is providing fraud awareness training to the relevant staff. Companies should devise and conduct fraud prevention and awareness workshops, which are focused on changing cultures and attitudes toward fraud by raising awareness. These workshops involve employees’ sensitization to probable fraud types and the warning signs and effective response training to fraud events.
Prevention is better than cure...

“The risk management team should be equipped with the necessary resources, skill sets and tools required to address the risk of fraud.”

2. Undertake comprehensive fraud risk assessment

Every organization has inherent and specific fraud risks that depend on factors such as industry, size, organization structure, internal controls environment, geographical location, etc. Organizations are increasingly considering fraud risk as a part of the companywide risk assessment programs to help them identify fraud risks and implement effective antifraud controls.

The key steps involved in this process are:

- Consideration of various types of fraud risks, viz., theft, employee fraud, fraudulent financial reporting, misappropriation of assets, etc.
- Consideration of various fraud schemes and scenarios unique to the industry/company
- Assessment of fraud risks at the overall company level, significant business unit level and significant account levels
- Mapping of existing controls and evaluation of effectiveness of controls
- Designing the implementation framework and monitoring mechanisms
- Conducting vulnerability reviews of various processes to the fraud risk and identifying areas where the anti-fraud controls are not working effectively
3. Implement adequate oversight/monitoring

- Adequate monitoring procedures should be established to review and improve the effectiveness of anti-fraud programs and controls. These may include:
  - Employees’ annual declaration on 100% compliance with the “code of business conduct and anti-fraud policies”
  - Adequate review/monitoring process to ensure that tip offs/complaints made through fraud hotlines are investigated/addressed appropriately
  - Oversight by the audit committee of the risk of override of controls by management

Testing the adequacy of preparedness to handle fraud risk:

In order to test whether the organization is adequately equipped to handle fraud risks or to respond to situations when fraud is uncovered, the following points will be useful:

- Have we documented a formal fraud policy and a code of conduct and ethics policy?
- Have we adequately and appropriately communicated the code of conduct and ethics policy?
- Do we have an effective whistleblower mechanism in place to enable the reporting of instances of observed/suspected instances of fraud?
- Have we trained our management team for the effective prevention and detection of fraud?
- Have we undertaken a fraud prevention health check to assess vulnerabilities to fraud?
- Does our risk assessment process specifically cover the risk of fraud?
- Is our internal audit team adequately equipped to cover the risk of fraud?
- Do we have an element of surprise in the internal audit process to deter fraud?
- Do we have adequate tools to detect suspicious or fraudulent transactions?
- Do we have the necessary skill sets to investigate fraudulent/dishonest acts?
More ways to stay connected to Ernst & Young

Assurance, Tax, Transactions, Advisory

We provide services to help you retain confidence of investors, manage your risk, strengthen your control and achieve your potential.

Read more on www.ey.com/Services

Center of excellence for key sectors

We have specialized teams that bring sector knowledge to you.

Read more on www.ey.com/industries

Publications – easy to use subscription form

www.ey.com/subscription-form

Webcasts and podcasts

http://webcast.ey.com/thoughtcenter/

The choice is yours!
Go to www.ey.com/india

Have questions about a specific EY service? Whatever your inquiry, we’ll help direct you to the right place.

www.ey.com
Our offices

Ahmedabad
2nd Floor, Shivalik Ishaan
Near CN Vidhyalaya
Ambawadi
Ahmedabad – 380 015
Tel:  + 91 79 6608 3800
Fax:  + 91 79 6608 3900

Bengaluru
“UB City”, Canberra Block
12th & 13th floor
No.24, Vittal Mallya Road
Bengaluru - 560 001
Tel:  + 91 80 4027 5000
Fax:  + 91 80 4219 4400

Chennai
TPL House, 2nd floor
No 3, Cenotaph Road
Teynampet
Chennai - 600 018
Tel:  + 91 44 4219 4400
Fax:  + 91 44 6632 8400

Hyderabad
205, 2nd floor
Ashoka Bhupal Chambers
Sardar Patel Road
Secunderabad - 500 003
Tel:  + 91 40 6627 4000
Fax:  + 91 40 2789 8851

Kolkata
22, Camac Street
Block ‘C’, 3rd floor
Kolkata – 700 016
Tel:  + 91 33 6615 3400
Fax:  + 91 33 2281 7750

Mumbai
6th floor & 18th floor
Express Towers
Nariman Point
Mumbai - 400 021
Tel:  + 91 22 6657 9200 (6th floor)
Fax:  + 91 22 2287 6401
Tel:  + 91 22 6665 5000 (18th floor)
Fax:  + 91 22 2282 6000

NCR
Golf View Corporate Tower - B
Near DLF Golf Course
Sector 42
Gurgaon – 122 002
Tel:  + 91 12 4646 4000
Fax:  + 91 12 4646 4050

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

For queries please contact:

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

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

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

Saket Bhartia
Associate Director
Direct: +91 80 4027 5670 Email:
saket.bhartia@in.ey.com
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 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

© 2011 Ernst & Young Pvt. Ltd. Published in India. All Rights Reserved.

In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

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.

EYIN1101-002 Artwork by Ritu Sharma