Monthly • Volume • XXXVIX • Page 1-58 • No.11 • November 2020

ICSI-NIRC NEWSLETTER

Insight

CYBER LAWS, FINANCIAL CRIMES, ARTIFICIAL INTELLIGENCE AND FORENSIC AUDIT

CONTENTS

Inside:

Motto
सत्यं वद। धर्मं चर।
speak the truth; abide by the law.

Vision
"To be a global leader in promoting good corporate governance"

Mission
"To develop high calibre professionals facilitating good corporate governance"

Published by :
CS Sonia Baijal, Regional Director for and on behalf of Northern India Regional council of the Institute of Company Secretaries of India, 4, Prasad Nagar Institutional Area, New Delhi-110005; E-mail: niro@icsi.edu; Phones: 493433000; Published at: NIRC-ICSI, 4, Prasad Nagar instl. Area, New Delhi.

NIRC-ICSI NEWSLETTER

» NIRC-ICSI Newsletter is generally published every month.
» Articles on subjects of interest to company secretaries are welcome.
» Views expressed by contributors are their own and the NIRC-ICSI does not accept any responsibility.
» The NIRC-ICSI is not in any way responsible for the result of any action taken on the basis of the advertisements published in the Newsletter.
» All rights reserved.
» No part of this newsletter may be reproduced or copied in any form by any means without the written permission of the NIRC-ICSI.
» The write-ups of the issue are also available on the website of the NIRC-ICSI.

"Winning doesn't always mean being first. Winning means you're doing better than you've done before."

- Bonnie Blair

Dear Esteemed Members & Students,

The start of November witnessed us all dealing with the uncanny situation created by the pandemic but since our doctors and scientists kept spinning faster and faster in the pursuit of the Covid-19 vaccine; the month finally led them near to having the vaccine in hands. I pray that soon we have a plan of implementation and action that makes our dream of overcoming this virus a reality.

At the outset, I sincerely want to appreciate and recognize each of you who has been a part of our NIRC team for keeping pace and putting enthusiastic efforts in successfully organizing, during November month, the MSOP and other academic and professional programs, Fit India: Fit ICSI Cycling campaign, master classes, knowledgeable webinars and once again setting the NIRC's records high. Combining my hopes with power of our NIRC's actions, I truly wish our upcoming All India Debate Competition and NCLT Moot Competition will have productive outcomes.

Further, I would like to thank my entire NIRC team for having come up with this Newsletter for the month of November. My genuine gratitude is extended to our professionals who come up with amazing write-ups every time and the readers who admire our Newsletters and it is an honour to bestow upon you all my cordial welcome to the NIRC's November, 2020 Newsletter.

The theme that we are presenting this time is: ***"CYBER LAWS, FINANCIAL CRIMES, ARTIFICIAL INTELLIGENCE AND FORENSIC AUDIT"***

Cyberspace is a place that is virtual, unreal and existing in the scope of internet without which it has

become impossible to imagine our lives. From making WhatsApp the new Suprabhatam to ordering food, grocery, clothes and even booking homes, hotels online, we have made ourselves the astronauts of cyberspace. Every appliance we use, from a washing machine to a car, has computing, and many these days can be connected to internet. It is not just a desktop or laptop computer or a mobile phone that provides the evolved cybercriminal a weapon. Cyber threats are constantly evolving in order to take advantage of online behaviour and trends.

"Cyberspace evolution is inevitable, and running away from it is definitely neither the answer to avoid harm nor is it really going to protect us."

It is with this inevitable online trend coupled with potential misdemeanors including financial and defamatory that cyber laws have evolved over time and are made responsible at most to create a safe and secure cyber environment for people.

Cyber Laws are the legislations focused on governing cyber space relating to legal informatics and supervision of digital circulation of information, software, information security and e-commerce. These laws cover many areas & activities occurring online and serve a variety of purposes. Some laws are formed to protect to defend people online from malicious activities, some laws explain the policies if using computers and the internet in a company. The wide range areas encompassing the cyber laws include scam, copyrighting issues, online character degradation, harassment and stalking, data protection, etc.

However, due to unrealistic and virtual nature of cyberspace as well as expertise of sophisticated criminals, the crimes committed are often invisible and it demands a logical flow of evidences to help the court in understanding them and the evidences presented. This demand can be served by doing forensic audit – a type of examination of financial records to unearth any illegal or fraudulent activity, conducted with the assumption that the findings may be used in court.

From regulators, banks and insurance companies to police personnel and lawyers, everybody wants to retain the services of forensic auditors these days. This area is one the fastest evolving fields possibly holding much scope in the profession of Company Secretary as well.

Coupled with accounting, auditing, investigative and technological skills and the knowledge of working of the legal system to establish facts and evidence in a court so that criminal acts such as siphoning of company funds, embezzlement or fraud are detected, a Company Secretary can try his hand in forensic audit and extract the best out of his own Company Secretary skills.

The month of December has already begun and this time it holds much of significance and proud moments for our Institute of Company Secretaries of India (ICSI) for it is the occasion of the biggest event of ICSI that is the 48th National Convention of the Company Secretaries to be held in Indore which is a home to cleanliness and has been ranked as the cleanest city for the fourth consecutive time adding to the glory of this event. With convenience of being a part of this event physically or through a virtual platform this time, I truly hope this year the Convention is going to unite the CS family more and will be marked memorable in the history of ICSI.

Also, by the time our Students receive this publication, I hope they would be dedicatedly dwelled in their studies. I convey my best wishes to all of you who are appearing for the December, 2020 Examinations. Sincere efforts coupled with consistent attitude will definitely yield desired results. Remember to study hard, no matter if it seems impossible, no matter if it takes time, no matter if you have to up all night, just remember that the feeling of success is the best thing in entire world.

Making way into further pages of this Newsletter, hope our readers immensely gain from the rest of it.

I look forward to receiving your valuable suggestions and feedback.

Do not hesitate to interact with me at chairman.nirc@icsi.edu

CS Suresh Pandey
Chairman-NIRC of ICSI
Chairman.nirc@icsi.edu
Mob. +91 9968300649

WEBINAR ON 'ECONOMIC REVIVAL THROUGH CAPITAL MARKETS POST COVID-19'

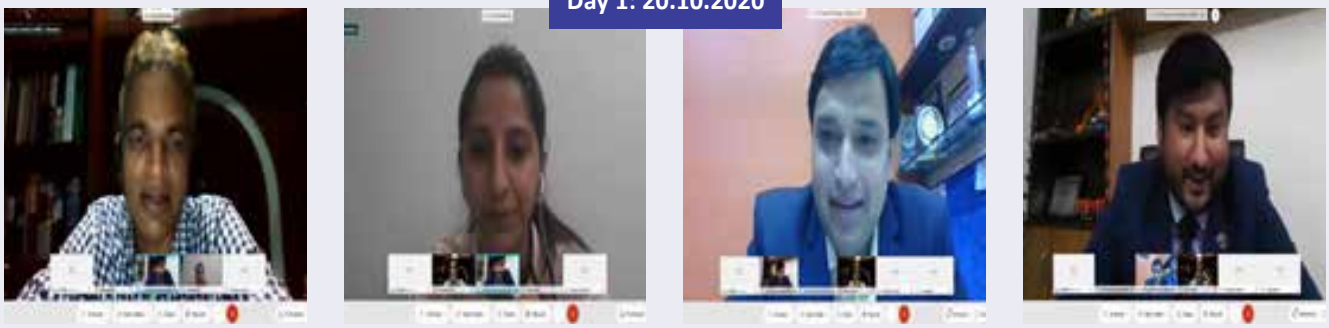
Dr. Jitendra Singh, Hon'ble Minister of State (Independent Charge), Ministry of Development of North Eastern Region; Minister of State, Prime Minister`s Office; Ministry of Personnel, Public Grievances and Pensions, Department of Atomic Energy and Department of Space, Government of India addressing the Participants. Also seen CS Ashish Garg, President, ICSI, CS Praveen Soni, Council Member, ICSI, CS Suresh Pandey, Chairman, NIRC-ICSI, Mr. J N Gupta, Former Executive Director, SEBI & Founder Stakeholders Empowerment Services and CS Sonia Baijal, Regional Director, NIRC-ICSI.

Mr. Anant Barua, Whole Time Member, SEBI, Mr. Prithvi Haldea, Founder Chairman, PRIME Database, Mr. J N Gupta, and Mr. Shaji Vikraman, Senior Journalist addressing the Participants.

Screen View: Dr. Jitendra Singh, Hon'ble Minister of NE State & PMO, CS Ashish Garg, CS Praveen Soni, CS Suresh Pandey, Mr. Anant Barua, Mr. Prithvi Haldea, Mr. J N Gupta, Mr. Shaji Vikraman and CS Sonia Baijal.

4 DAYS ONLINE MASTER CLASS ON RECENT AMENDMENTS IN CORPORATE LAWS FROM 20TH OCTOBER, 2020 TO 23RD OCTOBER, 2020

Day 1: 20.10.2020

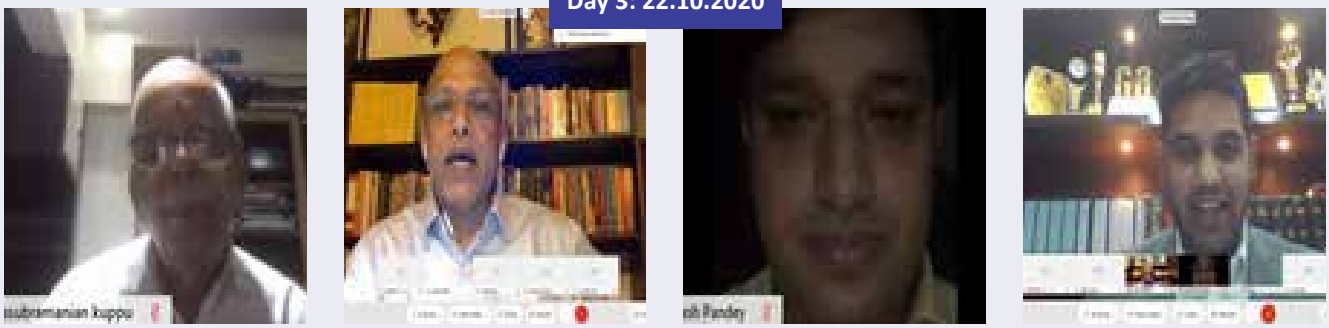


CS Vinod Kothari, Director, Vinod Kothari Consultants P. Ltd, CS Smriti Wadehra, Assistant Manager, Vinod Kothari Consultants P. Ltd, CS Suresh Pandey and CS Himanshu Harbola, Regional Council Member, NIRC-ICSI addressing the Participants.

Day 2: 21.10.2020

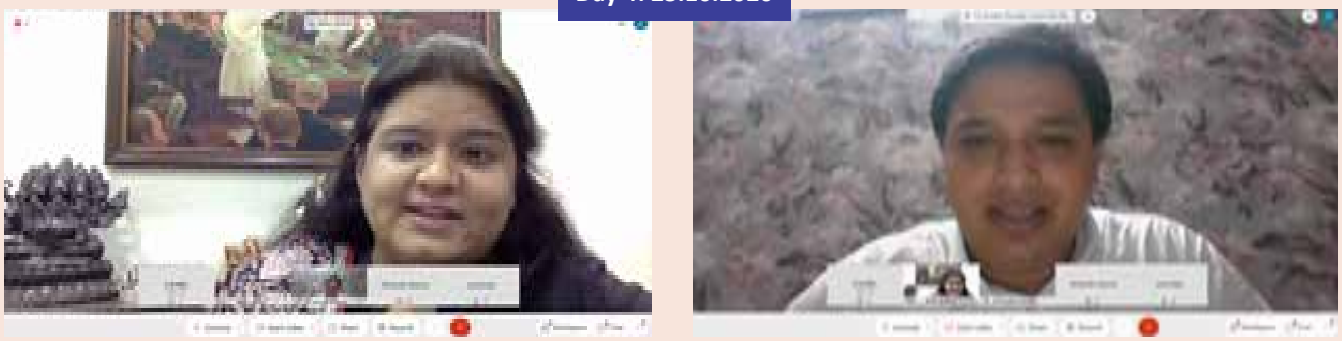
CS Shailashri Bhaskar, Practicing Company Secretary addressing the Participants. Also seen CS Suresh Pandey and CS Saurabh Kalia, Regional Council Member, NIRC-ICSI.

Day 3: 22.10.2020



Shri K. Ramasubramanian, General Manager (Rtd,), Reserve Bank of India, Mumbai & CA Anil Sharma, Former Independent Director, UCO Bank addressing the Participants. Also seen CS Suresh Pandey and CS Susshil Daga, Secretary, NIRC-ICSI.

Day 4: 23.10.2020



Ms. Raavi Birbal, Advocate, Supreme Court of India addressing the Participants. Also seen CS Suresh Pandey.

PUBLICATION

CS Ashish Garg receiving the Publication of Research Paper Writing Competition from CS Suresh Pandey alongwith CS Sonia Baijal and Dr Rajesh Gupta, Deputy Director, NIRC-ICSI

DIWALI PUJA

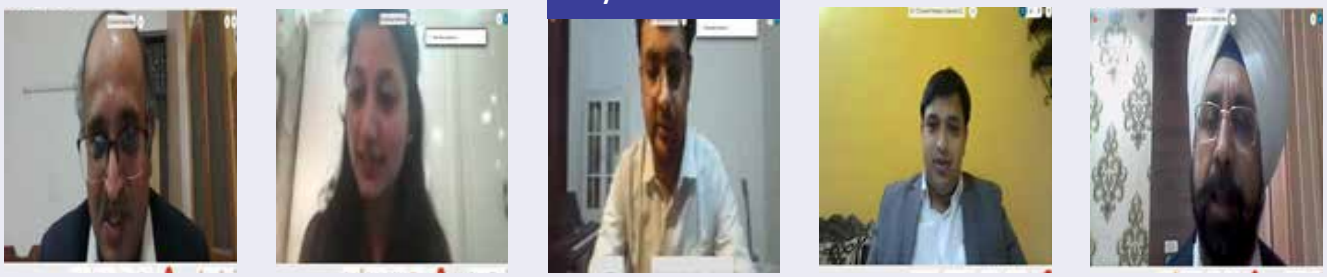
CS Manish Gupta Council Member ICSI, CS Suresh Pandey and CS Sonia Baijal During Diwali Puja at NIRC

OBSERVANCE OF VIGILANCE AWARENESS WEEK, 2020 'सतर्क भारत, समृद्ध भारत' - SATARK BHARAT, SAMRIDDH BHARAT (VIGILANT INDIA, PROSPEROUS INDIA)]

CS Suresh Pandey seen taking Pledge along-with Officials of NIRO

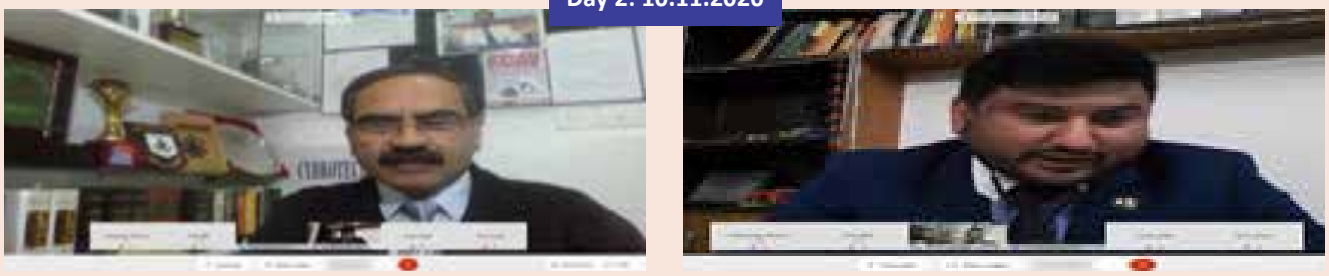
4 DAYS ONLINE MASTER CLASS ON CYBER LAWS, FINANCIAL CRIMES, ARTIFICIAL INTELLIGENCE AND FORENSIC AUDIT FROM 9TH NOVEMBER, 2020 TO 12TH NOVEMBER, 2020

Day 1: 9.11.2020



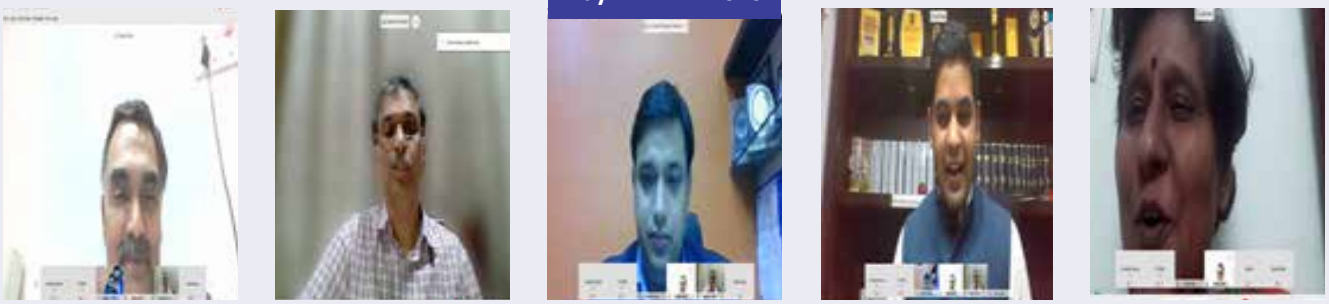
CS S Bhasker, Industry Principal, India Business Unit - Infosys Limited, Ms. Mimansa Ambastha, Cyber Lawyer, India Business Unit - Infosys Limited and Mr. Harshit Anant Mishra, Cyber Lawyer, India Business Unit - Infosys Limited addressing the Participants. Also seen CS Suresh Pandey and CS GS Sarin, Immediate Past Chairman, NIRC-ICSI

Day 2: 10.11.2020



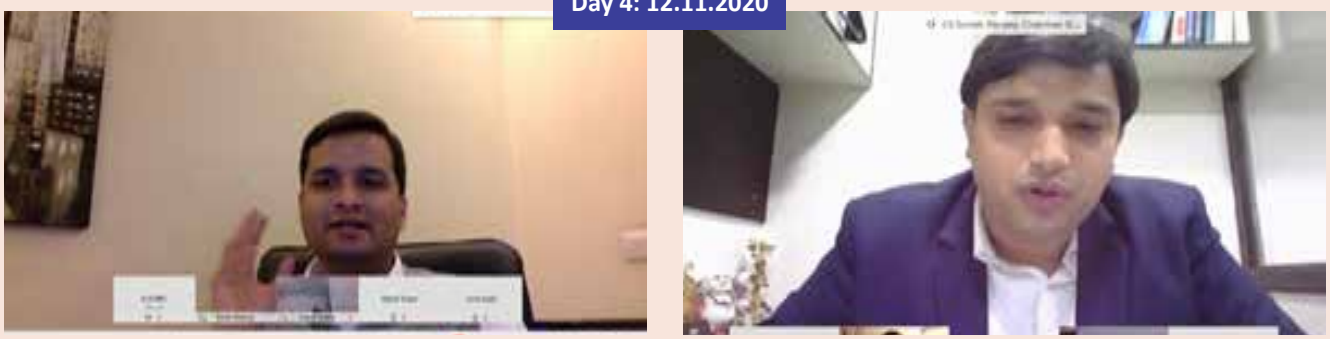
Mr. Anuj Agarwal, Chairman, Centre for Research on Cyber Crime and Cyber Law addressing the Participants. Also seen CS Himanshu Harbola.

Day 1: 11.11.2020



CA Chetan Dalal, Founder, CDIMS and CA Mahesh Bhatki, Director, CDIMS addressing the Participants. Also seen CS Suresh Pandey, CS Susshil Daga and CS Sonia Baijal.

Day 4: 12.11.2020



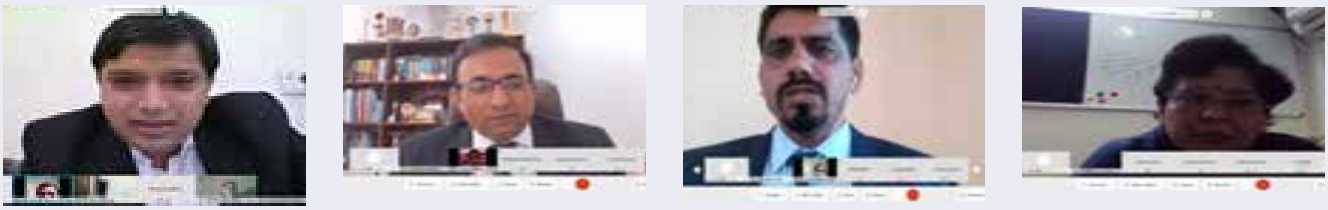
Mr. Kartik Sharma, Artificial Intelligence Practitioner addressing the Participants. Also seen CS Suresh Pandey.

VALEDICTORY FUNCTION – 3RD ONLINE MSOP (307TH BATCH)

Screen View: CS Suresh Pandey, CS Devender Suhag, Treasurer, NIRC-ICSI and CS Himanshu Harbola addressing the Participants during Valedictory Session.

Screen View of Participants of 3rd Online MSOP (307th Batch).

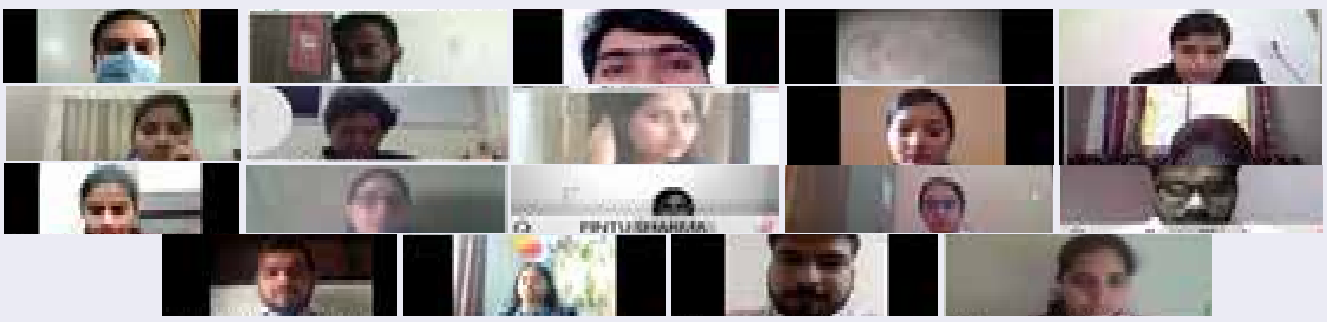
INAUGURATION FUNCTION – 4TH ONLINE MSOP (308TH BATCH)



Screen View: CS Suresh Pandey, CS Hitender Mehta, Council Member ICSI, CS Devender Suhag and CS Sonia Baijal, addressing the Participants during Inaugural Session.

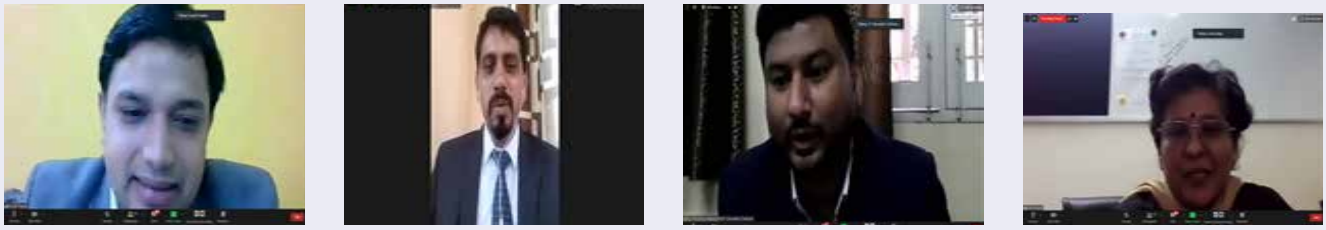
VALEDICTORY FUNCTION – 4TH ONLINE MSOP (308TH BATCH)

Screen View: CS Suresh Pandey, CS Devender Suhag and CS Sonia Baijal addressing the Participants during Valedictory Session.



Screen View of Participants of 4th Online MSOP (308th Batch).

INAUGURATION FUNCTION – 5TH ONLINE MSOP (309TH BATCH)

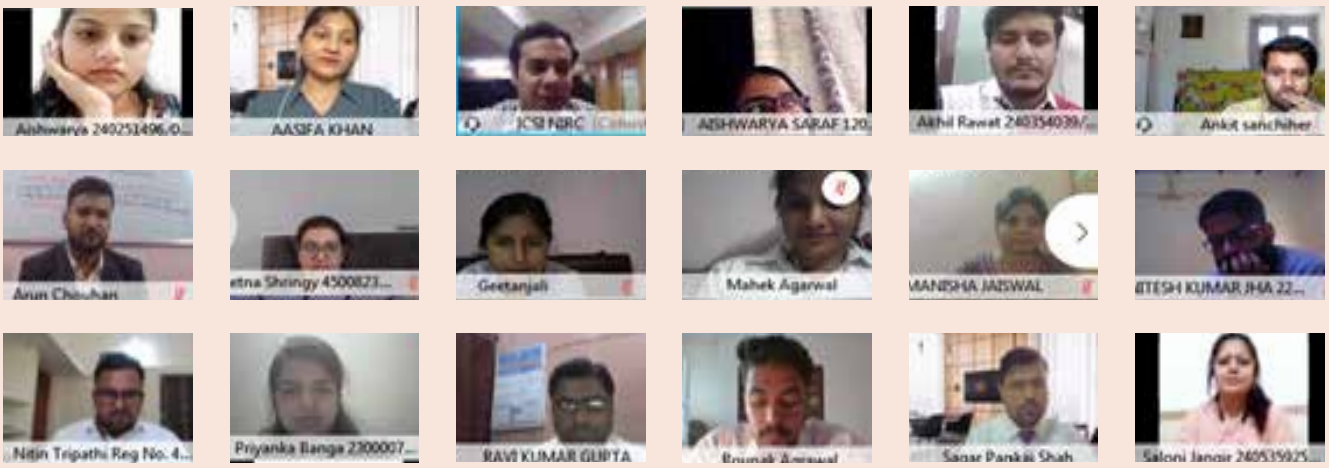


Screen View: CS Suresh Pandey, CS Devender Suhag, CS Himanshu Harbola and CS Sonia Baijal, addressing the Participants during Inaugural Session.

Screen View of Participants of 5th Online MSOP (309th Batch).

INAUGURATION FUNCTION – 6TH ONLINE MSOP (310TH BATCH)

Screen View: CS Suresh Pandey, CS Sonia Baijal and Dr. Rajesh Gupta addressing the Participants during Inaugural Session.



Screen View of Participants of 6th Online MSOP (310th Batch).

RECENT INITIATIVES TAKEN BY NIRC

Dear Friends,

I am pleased to enlist the recent initiatives for your kind information and ready reference:-

DIWALI PUJA

Diwali Puja was performed on 13th November, 2020 at NIRC Premises. Central Council, Regional Council members and officials of NIRO pray to Goddess Lakshmi and took her blessings for future endeavors.

CAPITAL MARKET WEEK -WEBINAR ON THE THEME 'ECONOMIC REVIVAL THROUGH CAPITAL MARKETS POST COVID-19'

With a view to commemorate Capital Market Week, NIRC organized Webinar on the theme 'Economic Revival through Capital Markets Post Covid-19' on Tuesday, the 3rd November, 2020. Dr. Jitendra Singh, Hon'ble Minister of State (Independent Charge), Ministry of Development of North Eastern Region; Minister of State, Prime Minister`s Office; Ministry of Personnel, Public Grievances and Pensions, Department of Atomic Energy and Department of Space, Government of India was the Chief Guest. He appreciated the efforts and contribution of the Institute, NIRC-ICSI in Nation Building. More than 6000 participants attended the live Program throughout the Country. Mr. Anant Barua, Whole Time Member, SEBI, Mr. Prithvi Haldea, Founder Chairman, PRIME Database, Mr. J N Gupta, Former Executive Director, SEBI & Founder Stakeholders Empowerment Services and Mr. Shaji Vikraman, Senior Journalist were the Guest Speakers. The Webinar witnessed rich deliberations and extensive exchange of thoughts on topic 'Making Capital Market more Investor Friendly'. The participants were given opportunity to raise their queries and the eminent speakers tried to resolve the maximum queries in the given time slot. The Webinar was well appreciated by the Participants.

4 DAYS ONLINE MASTER CLASS ON RECENT AMENDMENTS IN CORPORATE LAWS (15th Edition, Year 2020)

4 Days Online Master Class was orgnised by NIRC-ICSI on Recent Amendments In Corporate Laws from 20th October, 2020 to 23rd October, 2020. CS Vinod Kothari, Director, Vinod Kothari Consultants P. Ltd., CS Smriti Wadehra, Assistant Manager, Vinod Kothari Consultants P. Ltd., CS Shailashri Bhaskar, Practicing Company Secretary, Shri K. Ramasubramanian, General Manager (Rtd,), Reserve Bank of India, Mumbai, CA Anil Sharma, Former Independent Director, UCO Bank and Ms. Raavi Birbal, Advocate Supreme Court of India were the Guest Speakers at Master Class. The coverage included Companies (Amendment) Act, 2020, Recent Updates in Securities Laws, FEMA and Labour Laws. The Master Class was attended by around 200 Participants.

4 DAYS ONLINE MASTER CLASS ON CYBER LAWS, FINANCIAL CRIMES, ARTIFICIAL INTELLIGENCE AND FORENSIC AUDIT (16th Edition, Year 2020)

4 Days Online Master Class was orgnised by NIRC-ICSI on Cyber Laws, Financial Crimes, Artificial Intelligence and Forensic Audit from 9th November, 2020 to 12th November, 2020. CS S Bhasker, Industry Principal, India Business Unit - Infosys Limited, Ms. Mimansa Ambastha, Cyber Lawyer, India Business Unit - Infosys Limited, Mr. Harshit Anant Mishra, Cyber Lawyer, India Business Unit - Infosys Limited, Mr. Anuj Agarwal, Chairman, Centre for Research on Cyber Crime and Cyber Law, CA Chetan Dalal, Founder, CDIMS, CA Mahesh Bhatki, Director, CDIMS and Mr. Kartik Sharma, Artificial

Intelligence Practitioner were the Guest Speakers at Master Class. The coverage included Artificial Intelligence, Cyber Laws, Cyber Crimes and Investigations, Financial Crimes, Financial Frauds and Forensic Audit.

MOOT NCLT COMPETITION – 2020

ICSI-NIRC is conducting the first ever Moot NCLT Competition for Members & Students of ICSI through online mode. Each Team of Moot NCLT Competition will comprise of 2 Members & 1 Student. The Proposition will be based on Insolvency and Bankruptcy Code, 2016 & has been shared with Registered Participants only along with other necessary instructions. Winner of the competition shall be given 'Memento/Commendation Certificate'. The 1st Round of Moot NCLT held on 5th December, 2020.

RESEARCH PAPER PUBLICATION

The Publication having top 25 Research Papers was published and handed over to Shri Gopal Krishna Agarwal, National Spokesperson, Bharatiya Janata Party (Economic Affairs). He informed that hopefully the Innovative Ideas of Contributors may be used in the development of Nation. The Publication of Research Paper Competition was also handed over to CS Ashish Garg, President, ICSI and CS Ashis Mohan, Secretary, ICSI.

REVIEW MEETING OF LEADERSHIP SUMMIT 2020

Review Meeting of Leadership Summit 2020 held on 30th October, 2020 with CS Ashish Garg, President, ICSI and CS Ashis Mohan, Secretary, ICSI. Keeping in view of the present Pandemic situation, it was discussed to review the targets allocated to all the Regions and Chapters.

19th ALL INDIA DEBATE COMPETITION

ICSI-NIRC is hosting the 19th All India Debate Competition for students of the ICSI on the topic 'Effectiveness of Independent Directors on Corporate Boards'. Participation is restricted to the bonafide registered students of the ICSI.

ONLINE MANAGEMENT SKILL ORIENTATION PROGRAMME (MSOP)

NIRC-ICSI organized 4th Online Management Skill Orientation Programme (MSOP) (308th Batch of NIRC). The Inaugural Session held on 26th October, 2020. There were Real time online lectures in which participants directly interacted with the faculties throughout the 15 days of the MSOP.

The Valedictory of 3rd Online Batch held on 3rd November, 2020.

The Inaugural Session of 5th Online Management Skill Orientation Programme (MSOP) (309th Batch of NIRC) held on 10th November, 2020.

The Valedictory of 4th Online Batch held on 12th November, 2020.

The Inaugural Session of 6th Online Management Skill Orientation Programme (MSOP) (310th Batch of NIRC) held on 19th November, 2020.

VIRTUAL ALUMNI MEET OF PARTICIAPNTS OF MANAGEMENT SKILL ORIENTATION PROGRAMME (MSOP) AT NIRC OF ICSI IN THE YEAR 2019

The ICSI organized its first ever Alumni Meet (Virtual) for its newly inducted members OF Northern Region on 6th and 7th November, 2020. The Participants of the 1st Alumni Meet were the members who participated in the MSOP Batches at NIRC of ICSI in the year 2019. They

joined to enrich and perpetuate the bond with the institute and other members for mutual growth, support and benefit towards "problem solving and hand holding". It gave opportunity to newly inducted members to come together to Learn, Discuss and suggest.

ONLINE DEMO MEETING OF TOASTMASTERS INTERNATIONAL

NIRC-ICSI successfully conducted Demo Meeting of Toastmaster International on 31st October, 2020. The purpose was to improve the Public Speaking and Leadership Skills of the Students. Various students attended the online demo meeting.

15 DAYS ACADEMIC PROGRAM FOR STUDENTS

NIRC-ICSI organized Online 15 Days Academic Program for Students including 2 Days Induction Program, 3 Days e-Governance Program, 5 Days Skill Development Program and 5 Days Entrepreneurship Development Program. The students get the benefit of learning without moving out of their home and at the same time the sessions were live. This gives them liberty to clear their doubts and respond to the query raised by the faculties.

ONLINE EXECUTIVE DEVELOPMENT PROGRAM AND PDP

Keeping in view of the present Pandemic situation, NIRC is organizing back to back online Executive Development Program and PDP for the eligible students. Many students took advantage of online platform and completed their training programs.

ONLINE CRASH COURSE FOR EXECUTIVE AND PROFESSIONAL PROGRAMME STUDENTS

With a view to support students of Executive and Professional Programme for ensuing CS Examinations, NIRC has organized online Crash Course for Executive and Professional Programme students. Registration for online crash course is open for students interested in appearing for December, 2020 Examinations.

ONLINE CAREER AWARENESS PROGRAMS AND CAREER FAIRS

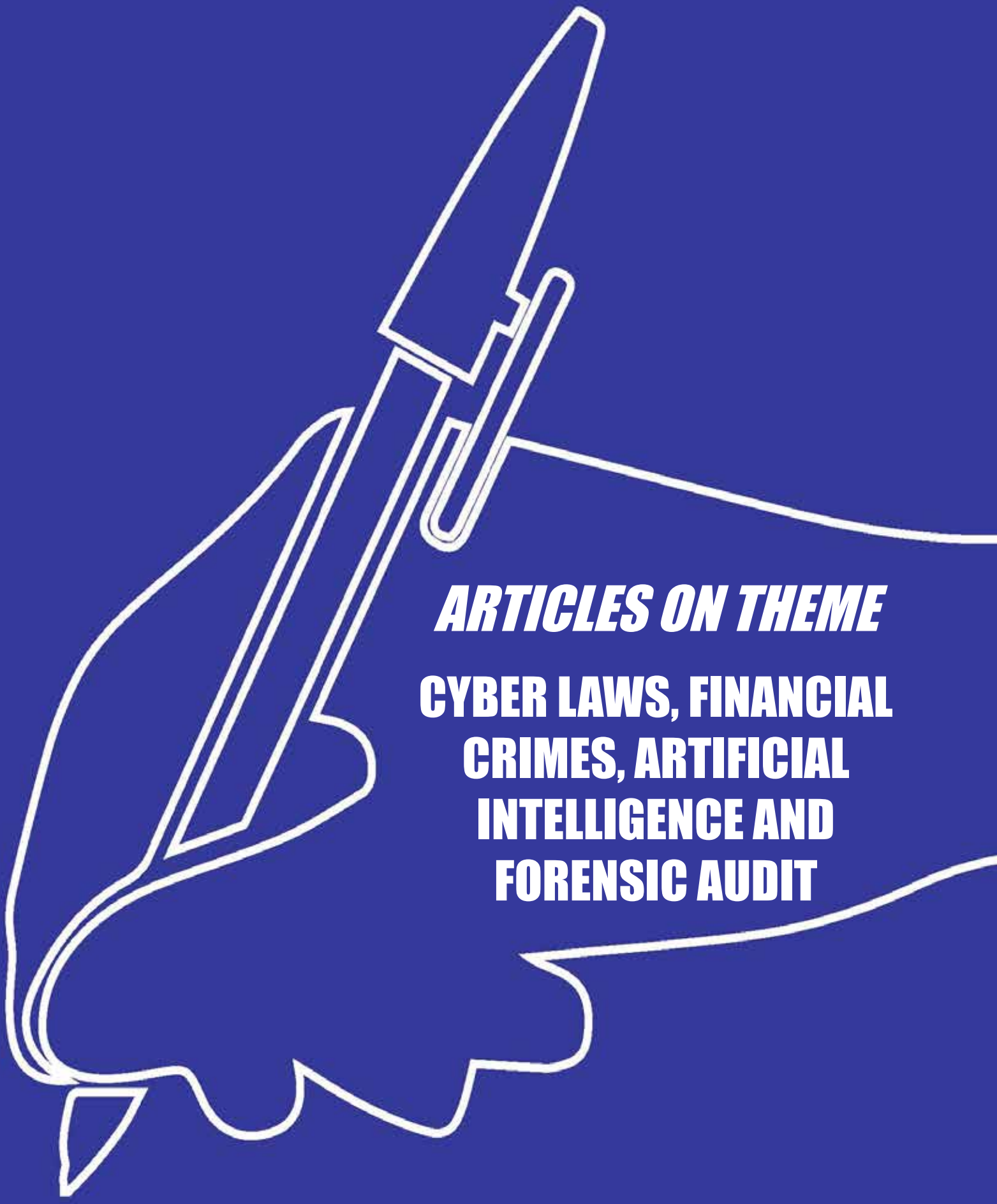
NIRC organized Online Career Awareness Programs for Students and Teachers of various Schools and Colleges. Further, NIRC also participated in online Career Fairs and apprised the students and their parents about the Role of Company Secretary, Company Secretary in Employment, Company Secretary in Practice and Eligibility, Validity and Cut-off Dates for Registration in CS. Many queries from Parents, Teachers and Students were also replied appropriately.

Friends, your feedback and participation is always welcome.

I am just a phone call away!

Yours own,

CS Suresh Pandey
Chairman-NIRC of ICSI
Chairman.nirc@icsi.edu
Mob. - +91 9968300649



ARTICLES ON THEME

CYBER LAWS, FINANCIAL CRIMES, ARTIFICIAL INTELLIGENCE AND FORENSIC AUDIT

Forensic Audit – What is it and how it is carried out

CS S K Gupta, FCS
cbst.skgupta@gmail.com

'if you see a fraud and do not say fraud, then you are a fraud'

- Naasim Nicholas Taleb

The perspective

With the increase in the financial frauds popularly known as white collar crimes, forensic auditing and accounting have risen to prominence. As per RBI data, in the last 11 fiscal years, 53,334 fraud cases were reported by banks involving Rs 2.05 lakh crores. Over 6,800 cases of bank fraud involving an unprecedented Rs 71,500 crore have been reported in 2018-19. A large number of frauds have surfaced in NBFC's (Recently, fraud identified in IL&FS),and in many other Private & Public companies and organisations also. The rigorous corporate governance norms and increasing stakes are prompting corporates to make sure that the board's have no blotches on their track record.

With reference to the "Darwin's theory of evolution", along with the humans, even crimes have evolved. These frauds or "White Collar Crimes" as they are more peculiarly known as, have revealed the extent to which they can adversely affect the corporate environment through corruption and fraudulent actions, which are beyond our imaginations. If there is one profession that is recession- as well as pandemic-proof in India, it is that of a 'forensic auditor'. From regulators, banks and insurance companies to police personnel and lawyers, everybody wants to retain the services of forensic auditors these days. Forensic audit is now a key weapon in every regulator's armoury and the moment one smells a scam or corporate wrongdoing, the brahmastra of 'forensic audit' is unleashed.

Major financial frauds – Some examples

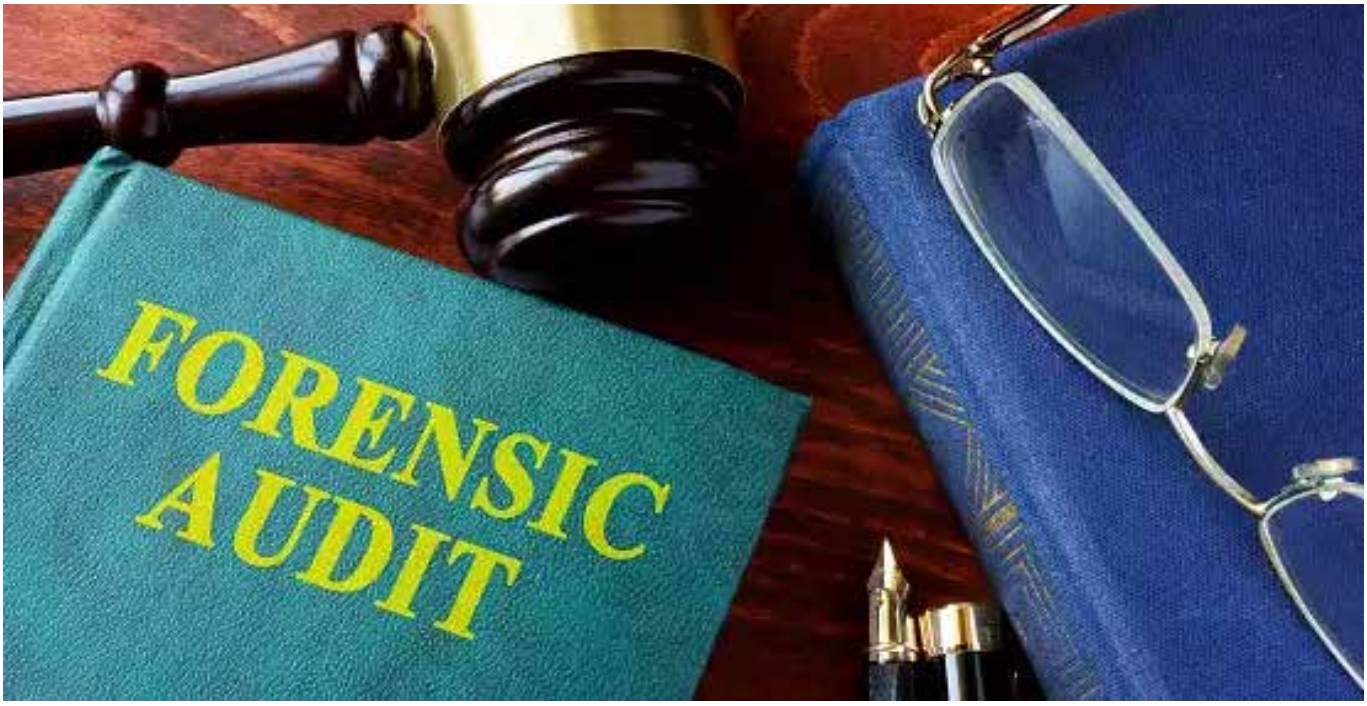
There is a rising trend of financial frauds the world over - McKesson and Robbins created fictitious sates and inventories. Great Salad Oil Swindle used the fact that oil and water do not mix to fraudulently over-state the quantity of oil in inventory tanks. The bottom part of the inventory tank was water and the top was salad oil. The auditors did not test all the way to the bottom of the tanks. Equity Funding was about fake insurance policies. Cedant Corporation was about fake revenues. Zzzz Best was a pyramid scheme. Sunbeam Corporation used what is called channel stuffing where revenue recognition is accelerated inappropriately. Nortel used what is called a big bath. Nortel had deferred recognition of expenses by recording as assets. This inflated total assets and total owners' equity. After several years, they wrote off the assets and recognized a huge loss that drove the owners' equity down. It washed away the profits. Worldcom also recorded assets when they should have recognized expenses. Enron is well known for using Special Purpose Entities to hide huge losses. Enron creatively and fraudulently recorded non-existent revenues. Qwest and Global Crossing used what are called swap sales to inflate reported income

What is Forensic Audit ?

If there is one profession that is recession- as well as pandemic-proof in India, it is that of a 'forensic auditor'. From regulators, banks and insurance companies to police personnel and lawyers, everybody wants to retain the services of forensic auditors these days. Forensic audit is now a key weapon in every regulator's armoury and the moment one smells a scam or corporate wrongdoing, the brahmastra of 'forensic audit' is unleashed.

Forensic Audit (FA) is an examination of evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court. FA is the process used

* The views expressed are personal views of the author and it should not be taken as views of the NIRC-ICSI



to examine an individual's or company's (including banking companies and other organisations) financial information for use as evidence in a court of law or legal proceedings. It is used to investigate fraud, embezzlement and other hidden irregularities. FA helps to detect diversion of funds, wilful defaults and window dressing of financial statements and helps to prosecute party for fraud, to determine negligence & for financial claims.

According to Collin Greenland, "Forensic accounting (or auditing) is the integration of accounting, auditing and investigative skills in order to provide an accounting analysis suitable for the resolution of disputes (usually but not exclusively) in the courts.

Business Dictionary defines Forensic Audit as the application of accounting methods to the tracking and collection of forensic evidence, usually for investigation and prosecution of criminal acts such as embezzlement or fraud. It further states that forensic audit is also called forensic accounting.

Dimensions of Forensic Auditing

Forensic Auditing is used in a number of ways and for a number of purposes and not just for criminal activity detection. Forensic Audit professionals dig deep into financial reports, locate financial transactions and figure out what really happened and who is the real culprit behind any fraud which has taken place in the company. Following are the broad dimensions of Forensic Auditing

- Frauds detection,
- Fraud detection and prevention techniques
- Investigation and analysis of financial evidence;
- Development of computerized applications to assist in the analysis and presentation of financial evidence;
- Communication of findings in the form of reports, exhibits and collections of documents;
- Assistance in legal proceedings, including testifying in court as expert witness and preparing visual aids to support trial evidence, etc.

Types of Frauds detected by Forensic Auditors

Forensic Auditors being the professionals carrying high degree of skepticism, effective probing techniques, highly analytical and well versed I documentation and evaluation usually detects the following types of frauds:

- Frauds related to Revenue and Sales- such as showing fictitious sales revenue(inflated/ deflated)
- Frauds with respect to falsifying the market position of the company by either showing false results or deceiving the shareholders by showing inflated share prices and consequently lower debts.
- Other frauds may also consist of various deceptive sale practices being undertaken by the company itself in order to capture market share or sustaining the present market position.

- Various third party frauds may also comprise of recording of deceptive allowances from vendors in order to falsify the revenue (inflated/ deflated) and even sometimes underachievement to vendors is also reported.
- Fraudulent acts of providing mis-statement in the financial statements by the directors such as no violation of law has taken place or Internal Financial Controls are in place etc.
- Frauds related to tampering of bank records and taking the monetary advantage thereof.
- Theft of competitor secrets or third party intellectual property rights may also amount to fraudulent act which also comes under the purview of forensic auditors.
- Various other frauds may also include-
  Showing financial statements as these are in line with the standards set or budgeted tasks.
  Falsifying the value of the business
  Using business resources for personal purposes
- Accepting bribes form the customers/ dealers/ vendors in order to facilitate business to them
- Representation of dummy workers/employees in the manpower sheets and consequently higher wage cost/ employee cost.
- Fictitious expenses and inflated incomes
- Showing dummy suppliers/ vendors and payments thereof
- Representing excess recoverable/ payables in the financial

Skills required by a Forensic Auditor

In addition to strong skills of accounting and auditing standards, procedures and related methodologies, forensic auditor must possess the following skills:

- Information Technology
- Data Analytics
- Criminology
- Legal Framework
- Litigation processes and procedures
- Investigation Techniques
- Evidence Gathering
- Network of professional contacts in related fields' viz. enforcement, regulatory bodies, law industry, peers etc.

Moreover, following are the key characteristics of Forensic Auditor-

- Strong visualisation, imagination and out of the box thinking
- Curiosity, creativity, discretion and scepticism
- Persistence, detail- oriented, inquisitiveness
- Confidence and sound professional judgement

Regulatory Stance on Forensic Audit

With the contemporary wave of making a New India in the year 2022 as free from corruption on the lines of good governance, Forensic auditing is a –

- Rapidly growing area as a specialized branch of accounting and investigations and
- Is concerned with the detection and prevention of financial fraud and white-collar criminal activities.

RBI has made forensic audit mandatory for large advances and cases involving restructuring of accounts. RBI has also operationalized a Central Fraud Registry which is a web based searchable database of frauds containing data for last 13 years. The Enforcement Directorate and the Serious Fraud Investigation Office have underscored the need for forensic audit following the rise in money laundering and wilful default cases that are plaguing the banking system.

Forensic Audit Procedure

Each Forensic Accounting assignment is unique. Accordingly, the actual approach adopted and the procedures performed will be specific to it. However, in general, many Forensic Accounting assignments will include the steps detailed below :

Step1. Initialization: It is vital to clarify and remove all doubts as to the real motive, purpose and scope of the assignment. It is helpful to meet the client to obtain an understanding of the important facts, players and issues at hand. A conflict check should be carried out as soon as the relevant parties are established. It is often useful to carry out a preliminary investigation prior to the development of a detailed plan of action.

Step 2. Develop Plan : This plan will take into account the knowledge gained by meeting with client and carrying out the initial investigation and will set out the objectives to be achieved and the methodology to be utilized to accomplish them.

Step 3. Obtain Relevant Evidence : Depending on the nature of the case, this may involve locating documents, economic information, assets, a person or company, and / or proof of the occurrence of an event. In order to gather detailed evidence,

the investigator must understand the specific type of fraud that has been carried out, and how the fraud has been committed. The evidence should be sufficient to ultimately prove the identity of the fraudster(s), the mechanics of the fraud scheme and the amount of financial loss suffered. It is important that the investigating team is skilled in collecting evidence that can be used in a court case and in keeping a clear chain of custody until the evidence is presented in court. If any evidence is inconclusive or there are gaps in the chain of custody, then the evidence may be challenged in court or even become inadmissible. Investigators must be alert to documents being falsified, damaged or destroyed by the suspect(s).

Step 4. Perform the analysis: The actual analysis performed will be dependent upon the nature of the assignment and may involve-calculating economic damages; summarizing a large number of transactions; performing a tracing of assets; performing present value calculations utilizing appropriate discount rates; performing a regression or sensitivity analysis; utilizing a computerized application such as a spread sheet, data base or computer model; and utilizing charts and graphics to explain the analysis.

Step 5. Reporting: Issuing an audit report is the final step of a fraud audit. Auditors will include information detailing the fraudulent activity, if any has been detected. The client will expect a report containing the findings of the investigation including a summary of evidence and a conclusion as to the amount of loss suffered as a result of the fraud. The report may include sections on the nature of the assignment, scope of the investigation, approach utilized, limitations of scope and findings and/or opinions. The report will include schedules and graphics necessary to properly support and explain the findings.

The report will also discuss how the fraudster set up the fraud scheme and which controls, if any, were circumvented. It is also likely that the investigative team will recommend improvements to controls within the organization to prevent any similar frauds occurring in the future. It should be kept in mind that the report should be based on the facts assimilated during the process and not on the opinion of the person writing the report.

Step 6. Court Proceedings: The investigation is likely to lead to legal proceedings against the suspect, and members of the investigative team will probably be involved in any resultant court case. The evidence gathered during the investigation will need to be presented at court, and team members may be called to court to describe the evidence they have gathered and to explain how the suspect was identified.

Approaches of Forensic Audit

1. Forensic Audit Thinking (Thinking Forensically)
2. Forensic Audit Procedures—both proactive and reactive
3. Forensic data analysis

The key elements are discussed in detail as below:

1. Forensic Audit Thinking: thinking forensically involves the critical assessment throughout the audit of all evidential matter and maintaining a higher degree of professional scepticism that, for example fraud or financial irregularity may have occurred, is occurring, or will occur in the future. Furthermore, Forensic thinking is a mind shift where the auditor believes that the possibility of fraud or financial irregularity may exist and the controls may be overridden to accomplish that possibility. Forensic thinking is used throughout the audit work

i.e. from start to finish.

2. Forensic Audit Procedures—both proactive and reactive Forensic audit procedures are more specific and geared toward detecting the possible material misstatements in financial statements resulting from fraudulent activities or error. Audit procedures should align with Fraud Risks and Fraud Risk Assessments.

Fraud Risks

Donald R. Cressy, in his proposition highlighted three interrelated elements that enable someone to commit fraud:

(a) The Motive that drives a person to want to commit the fraud,

(b) The Opportunity that enables him to commit the fraud, and

(c) The ability to rationalize the fraudulent behaviour.

Fraud Risk Assessment :

Fraud Risk assessment is a process aimed at proactively identifying and addressing an organization's vulnerabilities to internal and external fraud. It is a powerful proactive tool in the fight against fraud for any organization. A fraud risk assessment starts with an identification and prioritization of fraud risks that exist in the organization. It is important to think about a fraud risk assessment as an ongoing, continuous process, rather than just an activity.

Performing Forensic Procedures: Forensic Auditors need to have :

- an investigative mind-set that should be more than sceptical.
- an understanding of fraud schemes termed as occupational fraud (Corruption, Asset Misappropriation and Financial statement fraud).
- Experience in dealing with fraud issues.
- Knowledge of certain investigative, analytical, and technology-based techniques (Digital or computer forensics, e.g. how to gather, analyze and interpret data)
- Knowledge of legal processes.

Forensic Audit Techniques

While fraud detection techniques will not identify all fraud, the use of sound techniques can increase the likelihood that misstatements or defalcations will be discovered on a timely basis. Some of the techniques that a forensic auditor may use are listed below:

1. General Audit Techniques
2. Statistical & Mathematical Techniques
3. Technology based /Digital Forensics Techniques
4. Computer Assisted Auditing Techniques
5. Generalised Audit Software
6. Common Software Tool
7. Data Mining Techniques
8. Laboratory Analysis of Physical and Electronic Evidences
9. Red Flags & Green Flags

3. Forensic data analysis

Forensic Data Analysis (FDA) is a branch of Digital forensics. It examines structured data with regard to incidents of financial crime. The aim is to discover and analyse patterns of fraudulent activities. Data from application systems or from their underlying databases is referred to as structured data. Forensic data analysis focuses on uncovering patterns of fraudulent activity within a structured data environment while maintaining the integrity of the data for later use in a court of law. Forensic Data Analysis can be used to Prevent, detect and control fraud along with other irregularities. It is the process of gathering, summarizing, comparing and aggregating existing different sets of data that organizations routinely collect in the normal course of business with the goal of detecting anomalies that are traditionally indicative of fraud or other misconduct. The analytics processes used in forensic data analysis present an opportunity for companies to move from a reactive risk mitigation environment to a proactive one where lessons learned and information from advanced analytics tools can help improve systems, process security, as well as with compliance.

Conclusion

It has surely proved that auditors are not just watchdogs but can be bloodhounds also. And fraudsters shall now fear the bloodhounds. Forensic Audit is a very specialist type of engagement, which requires highly skilled team members who have experienced not only of accounting and auditing techniques, but also of the relevant legal framework. ■

ARTICLE

Forensic Audit – The Leading Path to Emergent Economy

CS Prateek Bhansali, FCS
csprateekbhansali@gmail.com

"Forensic Audit is application of financial skills and investigative mentality to unresolved issues, conducted within the contest of the rules of evidence."

–Bologna

As its name, nothing it is so, many persons assumes it as forensic science or criminology matter. Forensic Audit, another name is Forensic Accounting; it is concerned with accounting methods or procedures for collecting evidence of fraud, embezzlement and white collar crime.

It is a special branch of accounting; it requires a specific skill set for fraud detection. A forensic auditor checks internal control system of the company to identify any weaknesses in the controls designed to safeguard assets and to determine whether anyone in the company has exploited control weaknesses to misappropriate assets for personal gain, bribery, corruption, embezzlement, extortion, misappropriation, etc.

Forensic Audit - Why?

Sometime before, a joint research was conducted by Grand Thornton and ASSOCHAM; they concluded that money laundering, window dressing, financial reporting fraud and bribery are most common corporate frauds that happen in India. Forensic audit is now a key weapon in every regulator's armory and the moment one smells a scam or corporate wrongdoing, the brahmastra of 'forensic audit' is unleashed.

Nowadays, corporate frauds are one of the major hindrances to the inclusive and sustainable growth of the economy of India. As the corporate frauds rise, economy falls down. Corporate fraud schemes go beyond the scope of an employee's stated position, and are marked by their complexity and economic impact on the business, other employees and outside parties.

Report by Goldman Sachs on the Impact of PNB Scam on Indian Economy

It is stated that "To global investors, India's economy may seem a bit like a raw mango these days—enticing from a distance but bitter to taste; good for pickles, and not much more. That Goldman Sachs cut India's economic growth estimate from 8% to 7.6% for financial year 2019 may not be a surprise after the swell of bank scams that have washed over headlines in the last few weeks. The global investment bank has cited the $2 billion fraud at the state-run Punjab National Bank (PNB) among the reasons for slashing the projections for the world's fastest-growing major economy. It is feared that the fraud is just the beginning of a prolonged period of pain for the Indian economy. "Markets and investors are questioning whether the problem is more systemic," the analysts wrote in the note to clients.

Indeed, in the days following the revelation that billionaire jewellers, Nirav Modi and Mehul Choksi, duped India's second-largest government bank, the PNB stock has lost more than a quarter of its market value. Other public sector bank scrips have tumbled, too."

As reported time and again with various incidents like that of Nirav Modi in the early month of 2018, of Vijay Mallya, of Sahara Subrato Rao, of Satyam Computers, of 2G and alike, Corporate Scams are affecting the economic health of the companies time and again. With nearly over 250 scams in India since 1947, an approximate of 20.23 Trillion US Dollar loss has been reported in Corporate Scams in India.

Let's have a short look on Indian Corporate Scams –

Punjab National Bank

Punjab National Bank appointed a BDO to

* The views expressed are personal views of the author and it should not be taken as views of the NIRC-ICSI

conduct a forensic audit of jeweler Nirav Modi's companies, according to people directly briefed on the matter.

The bank issued a formal appointment letter to the Belgium-headquartered audit firm on February 27, 2018 to conduct a forensic audit in the scam wherein Modi, his uncle Mehul Choksi and their companies have been accused of defrauding the bank of as much as Rs 12,700 crore.12

In the starting of January, 2018, PNB informed the BSE (Bombay Stock Exchange) that it has detected some "fraudulent and unauthorized transactions" in one of its branches in Mumbai to the tune of $ 1771.69 million (approx.). Following the announcement, the share price of the state-owned bank plunged 10%.

Meanwhile, the Central Bureau of Investigation (CBI) received two complaints from PNB against billionaire diamantaire Nirav Modi and Jewellery Company alleging fraudulent transactions worth about Rs. 11, 400 crores, the Press Trust of India reported. This is in addition to the Rs. 280 crore fraud case that he is already under investigation for, again filed by PNB.

Nirav Modi, the billionaire in the middle of this controversy, is a luxury diamond jewelry designer who was ranked #85 in the Forbes list of India's billionaire in 2017.

- ✓ In a statement issued to stock exchanges, PNB said it has detected some "fraudulent and unauthorized transactions (messages)".
- ✓ A stock statement is a business statement that provides information on the value and quantity of stock related transactions. It details opening and closing balances for transacted items as well.
- ✓ According to the complaint filed by PNB with the CBI on January 28, the fraudulent issuance of Letters of Undertakings (LOU) was detected at the Mid Corporate branch, Brady House in Mumbai.

Forensic Audit Ordered on Dena Bank, OBC

Finance Ministry ordered forensic audit on Dena Bank, OBC in Rs. 437 cr. fraud. The Finance Ministry has ordered a forensic audit of Dena Bank and Oriental Bank of Commerce after some of their Mumbai-based branches allegedly misappropriated funds worth Rs. 437 crore, mobilised through fixed deposits.

Professional services firm KPMG in India has been given the mandate to undertake forensic investigations, sources close to the development said. The report is expected in a month's time. In the case of Dena Bank, the misappropriation was to the tune of Rs. 257 crore and related to funds mobilised from seven corporate. In Oriental Bank's case, it related to misappropriation of funds amounting to

Rs. 180 crore, reportedly belonging to the Jawaharlal Nehru Port Trust.

The Central Bureau of Investigation is already looking into the alleged fraud. The developments are disparate ones and took place at different times. But a common feature could be that they centered on mobilising deposits: fixed deposits/ bulk deposits. The incidents have again brought to the fore the weak risk management systems in public sector banks.

"The persons responsible have been taken to task; some disciplinary action is being taken. There are also some suspensions, some transfers…," said Financial Services Secretary GS Sandhu.

He was speaking on the sidelines of realty and banking conclave in Mumbai. Shri Sandhu added that the Finance Ministry would soon make it mandatory for all senior officers — Deputy General Managers and GMs — to undergo a compulsory risk management course before they are considered for promotions. He said these instances (of misappropriation) have happened at the lower/branch level because of lack of due diligence and non-adherence to norms or procedures.

Shri SL Bansal, Former CMD of Oriental Bank, told Business Line in New Delhi that the bank had furnished the necessary information to the forensic auditor. The incident in Oriental Bank of Commerce dated to February 2014 and the bank had swung into action early in March itself to nip the fixed deposit scam in the bud, said Shri Bansal. Of the initial amount of Rs. 180 crore, as much as Rs. 110 crore was immediately recovered and handed over to the original remitter, he added.

Role of CS as a Forensic Auditor

When talking the all compassing growth, economic growth is one of the significant spheres to be adhered with the premium practices of good governance and henceforth the glitches bugging the emerging growth of economy are tackled by the government at priority.

In this context among other things, Corporate Frauds are considered as one of the major challenges which are obstructing the growth of corporates as well as of economy as a whole.

Forensic Auditors can be engaged in Public Practice or employed by Insurance companies, banks, police forces, government agencies and other organizations. The Role of Company Secretary as a Forensic Auditor may be understood as follows:

1. Investigation in criminal proceedings

A Company Secretary has investigative accounting skills to examine the documentary and other documents to give his expert advice on the

matter. Forensic auditor could be called upon by the police to help them in criminal investigations which could relate to corporate.

2. Injury Claims

Where any loss is there due to result of personal injury, sometimes, insurance companies wants expert advice from a forensic auditor before deciding whether the claim is valid and amounts to pay.

3. Investigation of fraud

A Company Secretary can help in business investigation where funds tracing, assets recovery, forensic intelligence due diligence involved. The forensic expert undertakes a detailed review of the available documentary evidence and forms his/her opinion based on the information gleaned during the course of that review.

4. Expert Opinion

A Company Secretary sees and carefully examines the financial statements of corporate and use his expertise to trace whether there is any fraud committed.

5. Inspection

A Company Secretary may assist Police Authorities, Anti-Corruption Bureau and other investigation authorities in collecting evidences and other investigation purposes. For Example –

- ✓ Section 157 of Cr.P.C., 1973
- ✓ Section 17 and 18 of Prevention of Corruption Act, 1988
- ✓ Section 6 of The Bankers Books Evidence Act, 1891
- ✓ Section 78 of Information Technology Act, 2000
- ✓ Section 447 of the Companies Act, 2013; etc.

Fraud and Forensic Audit : An Introspect

The term 'forensic audit' covers wide range of investigative work which the professionals in practice could be asked to perform. The work would normally involve an investigation into the financial affairs of an entity and is often associated with investigations into alleged fraudulent activity.

It covers to the whole process of investigating a financial matter, including potentially acting as an expert witness, if the fraud comes to trial.

The investigation is likely to be similar in many ways to an audit of financial information, in that it will include a planning stage, a period when evidence is gathered, a review process, and a report to the client.

'Forensic auditing' refers to the specific procedures carried out in order to produce evidence.

Audit techniques are used to identify and to gather evidence to prove, for example, "how long the fraud has been carried out, and how it was conducted and concealed by the perpetrators."

Evidence may also be gathered to support other issues which would be relevant in the event of a court case. Such issues could include:

a. The suspect's motive and opportunity to commit fraud
b. Whether the fraud involved collusion between several suspects
c. Any physical evidence at the scene of the crime or contained in documents
d. Comments made by the suspect during interviews and/or at the time of arrest
e. Attempts to destroy evidence.

This way, it is proved that the tool of forensic audit is one of the strong tools in detecting the frauds, assisting financial stability and enduring economic growth of the nation under vision New India, 2022.

Conclusion

The numbers of fraudulent activities and ambiguous financial activities have been accelerating all over the world. Consequently, businesses are exposed to risk of fraudulent activities. With all of the recent corporate accounting scandals at Parmalat, Xerox Corporation and Satyam Computer Services and all the high profile corporate frauds at Enron, WorldCom, HealthSouth followed by Bernie's Madoff's colossal ponzi scheme, the media has made Forensic Accounting and Forensic Auditing into a growth industry.

Forensic audit has established itself as dynamic and strategic tool in combating corruption, financial crimes and frauds through investigations and resolving allegations of fraud and embezzlement. Thus, forensic audit was needed to detect the fraud in companies that suspected fraudulent transactions. ■

ARTICLE

Cyber Crimes in India: A Critical Analysis

CS Pradeep Kumar Ray, FCS
fcspkray@gmail.com

'One of the hot areas right now is tracking down cybercrime and cyber terrorism.'

–Daniel Humburger

INTRODUCTION

Cyber Crime is not defined in the Information Technology Act, 2000 nor in the National Cyber Security Policy, 2013 nor in any other regulation in India. In common parlance, cybercrimes are offences relating to computers, information technology, internet and virtual reality. These are unlawful acts wherein the computer is either a tool or a target or both. Cybercrime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

SIGNS OF CYBER CRIMES

Any crime with the help of computer and telecommunication technology or any crime where either the computer is used as an object or subject are signs of cybercrimes.Even a petty offence like stealing or pick pocket can be brought within the broader purview of cybercrime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cybercrime.

TYPES OF CYBER CRIMES

Different types of cybercrimes have evolved with the passage of time. These are as follows:

1) **Fraud:** Online frauds are on the rise. Hence cyber laws are made to protect citizens by identifying and preventing different kinds of online theft.
2) **Copyright:** Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.
3) **Defamation:** Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.
4) **Harassment and Stalking:** Cyber laws both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.
5) **Freedom of Speech:** Freedom of speech is an important area of cyber law. Cyber laws draw limits of free speech including laws that prohibit obscenity.
6) **Trade Secrets:** Companies doing businesses online often depend on cyber laws to protect their trade secrets. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.
7) **Contracts and Employment Law:** Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns
8) **Identity theft:** Personal information of a person is stolen with the purpose of using their financial resources or to take a loan or credit card in their name
9) **Cyberterrorism:** Well-planned attack strategies on the Government and corporate computer system; a threat of extortion or any kind of harm subjected towards a person, organization, group or state.

* The views expressed are personal views of the author and it should not be taken as views of the NIRC-ICSI

10) **Cyberbullying:** When a teenager or adolescent harasses,defames, or intimidates someone with the use of the internet, phone, chat rooms, instant messaging or any other social network then the person is said to be committing the crime of Cyberbullying. Same crime done by adults it is known as Cyberstalking.
11) **Hacking:** Getting access to other people's computers and passwords to use it for their own wrongful gain.
12) **Cyber Harassment:** Various kinds of harassment can and does occur in cyberspace, or through the use of cyberspace. It can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cybercrimes.

CATEGORIES OF CYBER CRIME

Cybercrime can be classified into the following categories:

1) Cyber Crimes against Persons
2) Cyber Crimes against Property
3) Cyber Crimes against Government
4) Some other Cyber Crimes

1) Cyber Crimes against a Person
a) Cyber stalking
b) Impersonation
c) Loss of Privacy
d) Transmission trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography,
e) Harassment with the use of computer

2) Cyber Crimes against Property
a) Unauthorized Computer Trespassing
b) Computer vandalism
c) Transmission of harmful programmes
d) Siphoning of funds from financial institutions
e) Stealing secret information & data
f) Copyright
g) unauthorized possession of computerized information.

3. Cyber Crimes against Government
a) Hacking of Government websites
b) Cyber Extortion
c) Cyber Terrorism
d) Computer Viruses

4. Some Other Cyber Crimes
a) Logic Bombs
b) Spamming
c) Virus, worms, Trojan Horse
d) E-Mail Bombing
e) E-Mail abuse etc.

CYBER CRIMES THROUGH COMPUTERS

Cybercrimes are done by criminals through computers which can be categorized in two ways

a) The Computer as a Target-using a computer to attack other computers.e.g. Hacking, Virus/ Worm attacks, DOS attack etc.
b) The computer as a weapon-using a computer to commit real world crimes.e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

ASPECTS OF CYBER CRIME

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as:

a. Unauthorized access & Hacking:-any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.
b. Trojan Attack:-The program that acts like something useful but does the things that are quiet damping. The programs of this kind are called as Trojans.
c. Virus and Worm attack:-A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.Programs that multiply like viruses but spread from computer to computer are called as worms.
d. E-mail & IRC related crimes:-

1. Email spoofing- Email that appears to have been originated from one source when it was actually sent from another source.
2. Email Spamming- Sending email to thousands and thousands of users - similar to a chain letter.
3. Sending malicious codes through email-E-mails are used to send viruses, Trojans, etc. through emails as an attachment or by sending a link of website which on visiting downloads malicious code.
4. Email bombing- It is characterized by abusers repeatedly sending an identical email message to a particular address.
5. Sending threatening emails
6. Defamatory emails

7. Email frauds
8. IRC (Internet Relay Chat) related

e. Denial of Service attacks

NEED TO FIGHT CYBERCRIME

Cyberspace is our common heritage that we have inherited in our life times from the benefits of ever growing technologies. It is the lifeline of the entire universe. Given its irreversible position today, it is the duty of every netizen to contribute toward making the said cyberspace free of any trouble or cybercrime.

HOW TO PREVENT CYBER CRIME?

Cybersecurity laws or cyber laws in India provide protection from cybercrime. However, prevention is always better than cure. Therefore, one should take the following steps to prevent a cybercrime:

a) Unsolicited text message – Upon receiving text messages from an unknown number, avoid responding to text messages or automated voice messages from an unknown number.

b) Downloads on the mobile phone - Download everything on the mobile phone from a trustworthy source only.

c) Rating and feedback - Always check for the seller's rating and feedback of customers for the seller. Be sure that you are checking current feedbacks. Also, beware of feedbacks that are 100% seller favoring or have an entry on the same date.

d) Personal Information Request - Never respond to any emails or calls asking for your card CVV or a mail containing an attachment, which requires you to click on embedded links.

LAWS THAT PENALISE CYBER CRIMES

Cyber Laws are regulated by Cyber Laws or Internet Laws which include the Information Technology Act, 2000 ("IT Act"), Information Technology (Amendment) Act, 2008 and the Indian Penal Code, 1860 ("IPC"). These laws penalise a number of cyber-crimes and unsurprisingly, there are many provisions in the IPC and the IT Act that overlap with each other. The offences and relevant penal sections on cybercrime are highlighted here in below:

CYBER ATTACK

S.No.	Nature of Complaint	Section and punishments under IT Act,2000 and IT Amendment Act, 2008	Section and punishment under other Laws
1.	Mobile phone lost/stolen		Section 379 IPC up to 3 years imprisonment or fine or both
2.	Receiving stolen computer/ mobile phone /data (data or computer or mobile phone owned by you is found in the hands of someone else	Section 66 B– Up to 3 years imprisonment or Rupees one lakh fine or both	Section 411 IPC – up to 3 years imprisonment or fine or both
3.	Data owned by you or your company in any form isstolen	Section 66 - Up to 3 years imprisonment or fine up to Rupees five lakh or both	Section 379 IPC up to 3 years imprisonment or fine or both
4.	A password is stolen and used by someone else for fraudulent purpose	Section 66C - Up to 3 years imprisonment or Rupees one lakh fine Section 66 D - Up to 3 years imprisonment or Rupees one lakh fine	Section 419 IPC – upto 3 years imprisonment or fine Section 420 IPC - upto 7 years imprisonment or fine
5.	An e-mail is read by someone else by fraudulently making use of password	Section 66 Up to 3 years imprisonment or fine up to Rupees five lakh or both	
6.	A bio metric thumb impression is misused	Section 66 Up to 3 years imprisonment or Rupees one lakh fine	

7.	An electronic signature of digital signature is misused	Section 66C -Up to 3 years imprisonment or Rupees one lakh fine	
8.	A Phishing e-mail is sent out in your name, asking for login credentials	Section 66 D - Up to 3 years imprisonment or Rupees one lakh fine	Section 419 IPC – upto 3 years imprisonment or fine
9.	Capturing, publishing or transmitting the image of a private area without any person's consent or knowledge	Section 66 E - Up to 3 years imprisonment or fine not exceeding Rupees two lakh or both	Section 292 IPC- upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequentconviction
10.	Tempering with computer source document	Section 65 - Up to 3 years imprisonment or fine upto rupees two lakh or both Section 66 of IT Act 2000 - Up to 3 years imprisonment or fine up to Rupees five lakh or both	
11.	Data Modification	Section 66 - Up to 3 years imprisonment or fine up to Rupees five lakh or both	
12.	Sending offensive messages through communication service , etc.		Section 500 IPC – upto 2 years or fine or both Section 504 IPC - upto 2 years or fine or both Section 506 IPC - upto 2 years or fine or both – if threat be to cause death or grievous hurt, etc. – up to 7 years or fine or both Section 507 IPC - upto 2 years along with punishment u/s 506IPC Section 508 IPC - upto1 years or fine or both Section 509 IPC - upto 1years or fine or both
13.	Publishing or transmitting obscene material in electronic form	Section 67– first conviction up to 3 years and 5 lakhs Second and subsequent conviction – upto 5 years and upto 10 lakhs	Section 292 IPC- upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequentconviction
14.	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Section 67– first conviction up to 3 years and 5 lakhs Second and subsequent conviction – upto 5 years and upto 10 lakhs	Section 292 IPC- upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction

15.	Publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Section 67 B– first conviction upto 5 years and upto 10 lakhs Second and subsequent conviction – upto 7years and upto 10 lakhs	Section 292 IPC- upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction
16.	Misusing a Wi-fi connection - if done against State	Section 66 - Up to 3 years imprisonment or fine up to Rupees five lakh or both Section 66F of IT ACT 2000 – life imprisonment	
17.	Planting a computer virus- if done against the State	Section 66 - Up to 3 years imprisonment or fine up to Rupees five lakh or both Section 66F of IT ACT 2000 – lifeimprisonment	
18.	Conducting a denial of service attack against a government computer	Section 66 - Up to 3 years imprisonment or fine up to Rupees five lakh or both Section 66F of IT ACT 2000 – lifeimprisonment	
19.	Stealing data from a government computer that has significance from national security perspective	Section 66 - Up to 3 years imprisonment or fine up to Rupees five lakh or both Section 66F of IT ACT 2000 – life imprisonment	
20.	Not allowing the authorities to decrypt all communication that passes through computer or network	Section 69– Imprisonment upto 7 years and fine	
21.	Intermediaries not providing access to information stored on their computer to the relevant authorities	Section 69– Imprisonment upto 7 years and fine	
22.	Failure to block web sites when ordered	Section 69 A –Imprisonment upto 7 years and fine	
23.	Sending threatening messages by e-mail		Section 504 IPC - upto 2 years or fine or both
24.	Word, gesture or act intended to insultthe modesty of awoman		Section 509 IPC – upto 3 years and also with fine
25.	Sending defamatory messages by e-mail		Section 500 IPC – upto 2 years or fine or both
26.	Bogus websites, cyber frauds	Section 66 D -Up to 3 years imprisonment or Rupees one lakh fine	Section 419 IPC – upto 3 years imprisonment or fine Section 420 IPC - upto 7 years imprisonment or fine

27.	E-mail spoofing	Section 66C -Up to 3 years imprisonment or Rupees one lakh fine	Section 465 IPC – upto 2 years or fine or both Section 468 IPC – upto 7 years imprisonment andfine
28.	Making a false document	Section 66 D -Up to 3 years imprisonment or Rupees one lakh fine	Section 465 IPC – upto 2 years or fine or both
29.	Forgery for purpose of cheating	Section 66 D -Up to 3 years imprisonment or Rupees one lakh fine	Section 468 IPC – upto 7 years imprisonment andfine
30.	Forgery for purpose of harming reputation	Section 66 D -Up to 3 years imprisonment or Rupees one lakh fine	Section 469 – upto 3 years and fine
31.	E-mail abuse		Section 500 IPC – upto 2 years or fine or both
32.	Punishment for criminal intimidation		Section 506 IPC - upto 2 years or fine or both – if threat be to cause death or grievous hurt, etc – upto 7 years or fine or both
33.	Copyright infringement	Section 66 - Up to 3 years imprisonment or fine up to Rupees five lakh or both	Section 63, 63B Copyright Act, 1957
34.	Theft of computer hardware		Section 379 IPC up to 3 years imprisonment or fine or both
35.	Online Sale of Drugs		NDPS Act
36.	Online Sale of Arms		Arms Act

A cyber attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cybercriminals use a variety of methods to launch a cyber attack, including malware, phishing, ransomware, denial of service, among other methods.

TYPES OF CYBER ATTACKS

An attack can be active or passive.An "active attack" attempts to alter system resources or affect their operation.A "passive attack" attempts to learn or make use of information from the system but does not affect system resources (e.g., wiretapping).An attack can be perpetrated by an insider or from outside the organization. Further cyber attacks form different types as follows:

1. Software supply chain attacks-The threat actor typically installs malicious code into legitimate software by modifying and infecting one of the building blocks the software relies upon.
2. Evasive phishing cyberattacks- Advanced socially engineered evasion techniques are bypassing email security solutions with greater frequency. A surge in sextortion scams and business email compromise (BEC), threatening victims into making a payment through blackmail or by impersonating others, respectively.
3. Evasive email scams include encoded emails, images of the message embedded in the email body, as well as complex underlying code that mixes plain text letters with HTML character entities. Social engineering techniques allow the scammers to fly safely under the radar of anti-spam filters and reach their target's inbox.
4. Clouds under attack: The growing popularity of public cloud environments has led to an increase of cyber attacks targeting resources and sensitive data residing within these platforms.
5. Mobile device attacks-Malicious actors are

adapting techniques and methods from the general threat landscape to the mobile world.

6. Syntactic attacks-Following three things attack an individual and establishment through emails, web browsers, chat clients, remote software, and updates.

a) Viruses-It is a self-replicating program that can attach itself to another program or file in order to reproduce. It can hide in unlikely locations in the memory of a computer system and attach itself to whatever file it sees fit to execute its code. It can also change its digital footprint each time it replicates making it harder to track down in the computer.

b) Worms-It does not need another file or program to copy itself; it is a self-sustaining running program. Worms replicate over a network using protocols.

c) Trojan horses-It is designed to perform legitimate tasks but it also performs unknown and unwanted activity. These can be imbedded in trial versions of software and can gather additional intelligence about the target without the person even knowing it happening.

7. Semantic attacks-It is the modification and dissemination of correct and incorrect information. To set someone into the wrong direction or to cover your tracks, the dissemination of incorrect information can be utilized.

CYBER ATTACK IS PREVENTABLE

Cyber attacks, despite their prevalence, can be prevented through:

- Maintain security hygiene
- Choose prevention over detection
- Cover all attack vectors
- Implement the most advanced technologies
- Keep your threat intelligence up to date

CONCLUSION

Although a crime free society exists only in illusion, there should be constant attempt of rules to keep the criminalities lowest. Especially in a society that is dependent more and more on technology, crime based on electronic law-breaking are bound to increase and the law makers have to go the extra mile compared to the impostors, to keep them at bay.Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users.Cyber attacks can be prevented if precautionary measures are taken before it is too late. ■

Cyber Laws, Financial Crimes, Artificial Intelligence and forensic Audit.

CS Shikha Saxena, ACS
shikhasaxena214@gmail.com

Cyber Laws, financial crimes, artificial intelligence and forensic audit. Are these inter-related? Yes, but the question arises how? Simple what do you prefer? Hard work or smart work? Usually everyone and specially the new generation always gives preference to smart work which accomplishes our task in minimum efforts hence we start living in a virtual world where we entirely depend upon cyberspace from ordering online food to grocery shopping to online classes to deal with all our financial matter. To solve our daily routine problems, we rely on artificial intelligence rather than on ourselves. Earlier this was an option but after this COVID-19 pandemic situation, we do not have an option but to entrust our lives on the webspace. Yes, they indeed made our lives very beautifully simple but sometimes we forget how dangerous it could be specially for those who are not aware of these cyberspaces working. According to a recent study of a Government agency, the Computer Emergency Response Team reported 3.13 lakh incidents of cybersecurity in 2019 alone. They show us a data, where it had been reported that none other than our daily routine applications are stealing and selling our personal data from us like Big Basket, Unacademy, Just Dial, even an anonymous security researcher revealed that the country's largest bank, State Bank of India left a server unprotected by failing to secure it with a password. And the funniest part is we live oblivious to all these things and keep promoting without knowing the consequences.

In India half of the population is not aware of how to protect our data from online fraud or even how they are committed. Still, India is a country where people easily got honey-trapped. So, it is far from their knowledge about financial crimes or how they can protect themselves through with available cyber laws in India who provides protection from these online frauds and financial crimes committed by companies or by an individual.

Yes, our basic lives revolve around internet and with the advancement of technology we are connected with Artificial intelligence in one way or another like SIRI and other application which pools our all information, which we searched online and while using other sources through which there are often chances of having financial crimes like electronic crime, bribery corruption, market abuse & Insider trading or money laundering, tax evasion, bank frauds, insurance fraud which may not sound dangerous under Indian Penal Code, 1860 but they have potential to shake the society adversely. These financial crimes took a toll from our society and to prevent from all these Government of India introduced different kind of laws and cyber law is one of them.

Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence, there is a need for Cyber laws in India which is governed by the Information Technology Act 2000. This act provides the legal framework to users for doing any kind of transaction. Some of the basic knowledge I would like to brief here which an individual must know.

Section 65: A person who intentionally conceals, destroys or alters any computer source code (such as programmes, computer commands, design and layout), when it is required to be maintained by law commits an offence and can be punished with 3 years' imprisonment or a fine of 2 Lakhs INR or both

Section 66: If a person fraudulently uses the password, digital signature or other unique identification of another person, he/she can face imprisonment up to 3 years or/and a fine of 1

* The views expressed are personal views of the author and it should not be taken as views of the NIRC-ICSI

Lakh INR.

Section 66E: If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge, the person is entitled to imprisonment up to 3 years of fine up to 2 Lakhs INR or both

Section 66F: A person can face life imprisonment if he/she denies an authorized person the access to the computer resource or attempts to penetrate/ access a computer resource without authorization, with an aim to threaten the unity, integrity, security or sovereignty of the nation. This is a non-bailable offence.

Section 43A: If a body corporate is negligent in implementing reasonable security practices which cause wrongful loss or gain to any person, such body corporate shall be liable to pay damages to the affected person.

These are some common examples that we need to know in our daily life routine.

While prosecuting any financial crime, online fraud in court we also have an option to conduct forensic audit. It is used to expose the illegal activities and all the evidence which are gathered via forensic audit is admissible in court. The term forensic audit is not only related to financial matter but it can be used for closure of business, bankruptcy filing disputes etc. We all have been aware about the Satyam Scam which shook the Indian economy, that time this concept of nascent but today it made a significant difference in the society. Cybercrime is unlawful acts wherein the computer is either a tool or a target or both.

So, it is necessary to know about the things that we use daily specially when our lives depend on it. The government provides all resources and creates an awareness campaign to beware of frauds and use technology wisely but in case if you get trapped in any of financial crimes then there is no need to panic. We have cyber laws and cherry on the top is forensic audit. It is an old saying that caution was exercised to reduce the tragedy. So, to conclude this article I would say artificial intelligence made a significant change in our lives positively as well as negatively. It is up to us how cautiously we use and aware of available laws in India which provide protection in every aspect. The more we are using technology, the faster the financial crime is increasing and even though we are unwillingly becoming part of it unknowingly. So being a good citizen, know your rights and laws which give protection in every aspect of live. ■

Cyber Laws, Financial Crimes, Artificial Intelligence and Forensic Audit

CS Parul Jain, ACS
csparulnishujain101212@gmail.com

Cyber Laws

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

IT law does not consist a separate area of law rather it encloses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce.

- Ministry of Electronic and Information Technology, Government of India

Cyber-crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber-crimes in two ways

The Computer as a Target: - using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon: - using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws.

Technical Aspects Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as:

Unauthorized access & Hacking:

Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

By hacking web server taking control on another

* The views expressed are personal views of the author and it should not be taken as views of the NIRC-ICSI

person's website called as web hijacking

Trojan Attack:

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. The name Trojan Horse is popular.

Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan.

TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

Virus and Worm attack:

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.

Programs that multiply like viruses but spread from computer to computer are called as worms.

E-mail & IRC related crimes:

i. **Email spoofing**

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. Please Read

ii. **Email Spamming**

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

iii. **Sending malicious codes through email**

E-mails are used to send viruses, Trojans, etc. through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

iv. **Email bombing**

E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

v. **Sending threatening emails**

vi. **Defamatory emails**

vii. **Email frauds**

viii. **IRC related**

Three main ways to attack IRC are: attacks, clone attacks, and flood attacks.

Denial of Service attacks:

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

Importance of Cyber Laws:

a) It covers all transaction over internet.
b) It keeps eyes on all activities over internet.
c) It touches every action and every reaction in cyberspace.

Area of Cyber Laws:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

Fraud: Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

Copyright: The internet has made copyright violations easier. In early days of online communication, copyright violations were too easy. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.

Defamation: When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

Harassment and Stalking: Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

Freedom of Speech: Freedom of speech is an important area of cyber law. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there

is a debate about whether their actions consist of permissible free speech.

Trade Secrets: Companies doing businesses online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.

Contracts and Employment Law: Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

Advantages of Cyber Law:

- Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
- It allows Government to issue notification on the web thus heralding e-governance.
- It gives authority to the companies or organizations to file any form, application or any other document with any office, authority, body or agency owned or controlled by the suitable Government in e-form by means of such e-form as may be prescribed by the suitable Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.

Financial Crime

Financial crime over the last 30 years has increasingly become of concern to governments throughout the world. This concern arises from a variety of issues because the impact of financial crime varies in different contexts. It is today widely recognized that the prevalence of economically motivated crime in many societies is a substantial threat to the development of economies and their stability.

Financial crime is defined as crime that is specifically committed against property. These crimes are almost always committed for the personal benefit of the criminal, and they involve an illegal conversion of ownership of the property that is involved. Financial crimes can occur in many different forms, and they happen all over the world. Some of the most common crimes facing the financial sector are money laundering, terrorist financing, fraud, tax evasion, embezzlement, forgery, counterfeiting, and identity theft.

It is possible to divide financial crime into two essentially different, although closely related, types of conduct.

First, there are those activities that dishonestly generate wealth for those engaged in the conduct in question. For example, the exploitation of insider information or the acquisition of another person's property by deceit will invariably be done with the intention of securing a material benefit. Alternatively, a person may engage in deceit to secure material benefit for another.

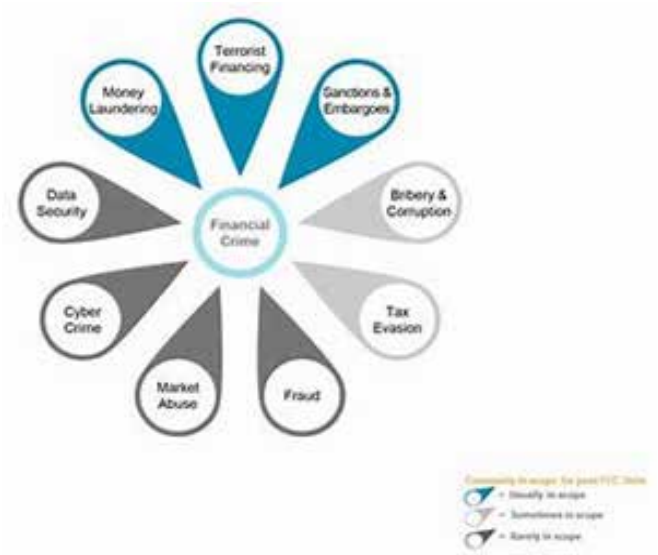
Second, there are also financial crimes that do not involve the dishonest taking of a benefit , but that protect a benefit that has already been obtained or to facilitate the taking of such benefit.

Commitment of Financial Crime

There are essentially seven groups of people who commit the various types of financial crime:

- ❖ Organized criminals, including terrorist groups, are increasingly perpetrating large-scale frauds to fund their operations.

- Corrupt heads of state may use their position and powers to loot the coffers of their (often impoverished) countries.
- Business leaders or senior executives manipulate or misreport financial data in order to misrepresent a company's true financial position.
- Employees from the most senior to the most junior steal company funds and other assets.
- From outside the company, fraud can be perpetrated by a customer, supplier, contractor or by a person with no connection to the organization.
- The external fraudster is colluding with an employee to achieve bigger and better results more easily.
- The successful individual criminal, serial or opportunist fraudsters in possession of their proceeds are a further group of people who have committed financial crime.



Types of Financial Crime

Financial crime is commonly considered as covering the following offences:

- fraud
- electronic crime
- money laundering
- terrorist financing
- bribery and corruption
- market abuse and insider dealing
- information security

Link between Financial crime and terrorist financing

Terrorist organizations require financial support in order to achieve their aims and a successful terrorist group, like any criminal organization, is therefore one that is able to build and maintain an effective financial infrastructure.

It is generally believed that terrorist organization raise funds by the following means:

Llegitimate sources, such as the abuse of charities or legitimate businesses self-financing (i.e. through their members or sympathizers), criminal activity, state sponsors and activities in failed states and other safe heavens

Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move these funds between jurisdictions. To manage their finances, they draw on the services of professionals, such as bankers, accountants and lawyers, and take advantage of a range of financial services products.

Artificial Intelligence (AI)

Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. The term may also be applied to any machine that exhibits traits associated with a human mind such as learning and problem-solving.

The ideal characteristic of artificial intelligence is its ability to rationalize and take actions that have the best chance of achieving a specific goal.

Artificial intelligence is based on the principle that human intelligence can be defined in a way that a machine can easily mimic it and execute tasks, from the simplest to those that are even more complex. The goals of artificial intelligence include learning, reasoning, and perception.

AI is continuously evolving to benefit many different industries. Machines are wired using a cross-disciplinary approach based in mathematics, computer science, linguistics, psychology, and more.

Algorithms often play a very important part in

the structure of artificial intelligence, where simple algorithms are used in simple applications, while more complex ones help frame strong artificial intelligence.

Applications of Artificial Intelligence

The applications for artificial intelligence are endless. The technology can be applied to many different sectors and industries. AI is being tested and used in the healthcare industry for dosing drugs and different treatment in patients, and for surgical procedures in the operating room.

Artificial intelligence also has applications in the financial industry, where it is used to detect and flag activiti in banking and finance such as unusual debit card usage and large account deposits—all of which help a bank's fraud department. Applications for AI are also being used to help streamline and make trading easier. This is done by making supply, demand, and pricing of securities easier to estimate.

Categorization of Artificial Intelligence

Artificial intelligence can be divided into two different categories: weak and strong.

Weak artificial intelligence embodies a system designed to carry out one particular job. Weak AI systems include video games such as the chess.

Strong artificial intelligence systems are systems that carry on the tasks considered to be human-like. These tend to be more complex and complicated systems. They are programmed to handle situations in which they may be required to problem solve without having a person intervene. These kinds of systems can be found in applications like self-driving cars or in hospital operating rooms.

Special Considerations

Since its beginning, artificial intelligence has come under scrutiny from scientists and the public alike. One common theme is the idea that machines will become so highly developed that humans will not be able to keep up and they will take off on their own, redesigning themselves at an exponential rate.

Another is that machines can hack into people's privacy and even be weaponized. Other arguments debate the ethics of artificial intelligence and whether intelligent systems such as robots should be treated with the same rights as humans.

Self-driving cars have been fairly controversial as their machines tend to be designed for the lowest possible risk and the least casualties. If presented with a scenario of colliding with one person or another at the same time, these cars would calculate the option that would cause the least amount of damage.

Another contentious issue many people have with artificial intelligence is how it may affect human employment. With many industries looking to automate certain jobs through the use of intelligent machinery, there is a concern that people would be pushed out of the workforce. Self-driving cars may remove the need for taxis and car-share programs, while manufacturers may easily replace human labor with machines, making people's skills more obsolete.

Forensic Audit

A forensic audit, also known as forensic accounting, refers to the application of accounting methods for detection and gathering evidence of frauds, embezzlement, or any other such white-collar crime. It is the application of accounting skills to legal questions.

A forensic audit is an examination and evaluation of a firm's or individual's financial records to derive evidence that can be used in a court of law or legal proceeding. Forensic auditing is a specialization within the field of accounting, and most large accounting firms have a forensic auditing department. Forensic audits require the expertise of accounting and auditing procedures as well as expert knowledge about the legal framework of such an audit.

Forensic audits cover a wide range of investigative activities. A forensic audit may be conducted to prosecute a party for fraud, embezzlement, or other financial crimes. In the process of a forensic audit, the auditor may be called to serve as an expert witness during trial proceedings. Forensic audits could also involve situations that do not involve financial fraud, such as disputes related to bankruptcy filings, business

closures, and divorces.

Difference between a financial audit and forensic audit

Engaging an audit is an important strategy to run a business, and all business-owners should know to identify the times when an audit is needed. However, forensic auditing is not the same as financial audit, both in terms of objective and procedure, leaving no scope for overlap.

- ✓ A financial audit is aimed at mere examination of the entity's financial statement, and adds credibility to the reported financial position and performance of a business. However, the object of a forensic audit is much beyond that.
- ✓ Forensic audit/accounting is a specialized branch of accounting, that requires a specialized skill set for fraud detection. A forensic auditor examines a company's system of internal controls to identify any weaknesses in the controls designed to safeguard assets and to determine whether anyone in the company has exploited control weaknesses to misappropriate assets for personal gain, including corruption, bribery, extortion, embezzlement, misappropriation, etc. It adds a legal substance to the auditing procedure.

Thus, where a financial audit is done, and there is a suspect-asset-fraud, a forensic audit is done to identify that.

Forensic Auditors and their roles

Forensic auditors/accountants do not differ from other financial accountants. However, they possess special skills to detect fraud, and ways to document it. Their role goes beyond just looking into statements, that includes investigation, bringing out evidence, writing reports, understanding the legal scope of the evidence, and ways to prove it in court. Thus, a forensic auditor is need of a little more professional skepticism and has to conduct critical assessment throughout the audit of all essential material, which is known as forensic thinking. It can be understood that the work of a forensic auditor is two-phased.

Investigation Services – At first the auditor begins with an investigation; looking into the accounts and statement, and identifying defects in it. It then moves on to find ways to deal with such defects, which is a reactionary function.

Litigation Services – It is entirely possible that the frauds detected be resolved within the company itself. However, there are times when they need to be resolved through legal channels. During such situations, forensic auditors give litigation support to the advocates. Their advice and consultation about the legalities of commercial disputes are very essential. Moreover, they also provide research assistance by giving relevant documents and facts to support a legal claim, and also help decide the extent of damage that is required. They are also called up by the Court as an expert witness for further investigation.

Types of Investigation

Corruption

Corruption is a major obstacle at corporate levels, and also to socio-economic development. It has far-reaching consequences, even total closure of the company.

Bribery – It refers to dishonestly influencing one's role/ position to receive something, and at the same time promising something favorable to the party proving such benefit.

Extortion – Taking a step ahead from bribery, extortion involves the use of threat, force or violence to extract money from another party/ person.

Conflict of interest – On a related note, anything, including bribery, that is done with the intention to gain personal benefit, and which is detrimental to the company, forms the objective of a forensic audit.

How is forensic auditing investigation conducted?

The process of a forensic audit is similar to a regular financial audit—planning, collecting evidence, writing a report—with the additional step of a potential court appearance.

Step 1 – Accepting the Investigation

A forensic audit is always assigned to an independent firm/group of investigators in order to conduct an unbiased and truthful audit and investigation.

Step 2 – Planning the Investigation

Planning the investigation is the key step in a forensic audit. The auditor(s) must carefully

ascertain the goal of the audit so being conducted, and to carefully determine the procedure to achieve it, through the use of effective tools and techniques.

Step 3 – Gathering Evidence

In forensic auditing specific procedures are carried out in order to produce evidence. Audit techniques and procedures are used to identify and to gather evidence to prove.

The investigators can use the following techniques to gather evidence:

- Testing controls to gather evidence which identifies the weaknesses, which allowed the fraud to be perpetrated
- Using analytical procedures to compare trends over time or to provide comparatives between different segments of the business
- Applying computer-assisted audit techniques, for example, to identify the timing and location of relevant details being altered in the computer system
- Discussions and interviews with employees
- Substantive techniques such as reconciliations, cash counts and reviews of documentation.

Forensic Data Analysis (FDA)

FDA is the technology used to conduct fraud investigations; the process by which evidence is gathered, summarized and compared with existing different sets of data. The aim here is to detect any anomalies in the data and identify the pattern of such anomalies to indicate fraudulent activity. Such an analysis requires three kinds of expertise.

Step 4 – Reporting

The reporting stage is the most obvious element in a forensic audit. After investigating and gathering evidence, the investigating team is expected to give a report of the findings of the investigation, and also the summary of the evidence and conclusion about the loss suffered due to the fraud.

Step 5 – Court Proceedings

The last stage expands over those audits that lead to legal proceedings. Here the auditors will give litigation support as mentioned above. The auditors are called to Court, and also included in the advocacy process.

Regulatory Authorities

● Reserve Bank of India

The Reserve Bank of India has made forensic audits mandatory for large advances and restructuring of accounts. In light of this, the RBI recently came up with the concept of creating a 'forensic audit pool.'

Also, by mandating forensic audits, the RBI operationalized a Central Fraud Registry (CFR), a web-based searchable database of frauds containing data for the last 13 years, in January 2016.

● Enforcement Directorate (ED)

The ED is a law enforcement agency and economic intelligence agency responsible for enforcing economic laws and fighting economic crime in India. It is part of the Department of Revenue, Ministry of Finance. It comprises officers of the Indian Revenue Service, Indian Police Service and the Indian Administrative Service.

Legal consequences that a person will attract if he/she is caught in a forensic audit

In order to understand the legal consequences that a person attracts on being caught in a forensic audit, it is necessary to know about the various

statutes that talk about the implementation of forensic audits in India.

Sections 235 and 237 of the Companies Act, 1956- Empowers the Central Government to inspect the books of accounts of a company, to direct special audit, to order an investigation into the affairs of a company and to launch prosecution for violation of the provisions of the Act.

Section 424A (5) of the Companies Act, 1956 empowers National Company Law Tribunal (NCLT) to examine as a preliminary issue whether the company is a sick industrial company u/s. 2(46AA).

Section 424B of the Companies Act, 1956 empowers the tribunal to make such inquiry as it may deem fit for determining whether any industrial company has become a sick industrial company.

SEBI Act, 1992- Regulation 11 C of the SEBI Act, 1992 empowers the SEBI to direct any person to investigate the affairs of intermediaries or brokers associated with the securities market whose transactions in securities are being dealt with in a manner detrimental to the investors or the securities market.

Insurance Act, 1938- Section 33 of the Act empowers the IRDA to direct any person (Investigating Authority) to investigate the affairs of any insurer.

Prevention of Money-Laundering Act, 2002– Section 3 of the Act defines the offence of money laundering as the involvement of a person in any process or activity connected with the proceeds of crime and projecting it as untainted property, where the scope of integrating forensic audits can be clearly seen.

The Companies (Auditor's Report) Order, 2003- The Act requires the auditor to report to the effect that if a substantial part of fixed assets has been disposed of off during the year, whether it has affected the going concern status. ■

"Cyber Laws :- Digital Safeguard against Internet Frauds"

CS Lalit Rajput, ACS
lalitrajput537@gmail.com

Cyber Laws refer to the term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. Cyber Laws provide legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and also provide a legal framework to mitigate, check cyber crimes. These laws are formed by keeping several issues into consideration such as our society, morals, computer ethics, etc.

Cyber law provides legal protections to people using the internet including both businesses and regular citizens and applied to the internet and internet-related technologies only.

Importance of Cyber Laws:

In this global Era, Information Technology is changing rapidly and gaining popularity in most of our aspects of lives. We are very much dependent upon technology and technical tools. Computer, Laptops, Mobile Phones, and Internet Facilities play an important role in today's global era, but that also includes the people involving in the commission of crimes using internet and technology. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence we need Specific Laws to cater these activities and therefore Cyber Laws (commonly known as Information Technology Act) was notified.

"The Cyber Laws in India has paved the way for electronic commerce and electronic governance in the country by ensuring maximum connectivity and minimum cybersecurity risks. Also, enhancing the scope and expanding the use of digital mediums," says Advocate Krishnamohan K Menon.

Governing Law(s) in India:

Cyber Laws in India prevent any crime done using technology. Cyber laws in India is not a separate legal framework. It's a combination of Contract, Intellectual property, Data protection, and privacy laws. The Indian cyber laws are primarily governed by the Information Technology Act (IT Act), penned down back in 2000 as amended from time to time and rules and regulations thereof. IT Act, 2000 addresses the gamut of new-age crimes. Computer technology, mobile devices, software, and the internet are both medium and target of such crimes.

Types of Cyber Crimes in India:

- **Identity theft -** When personal information of a person is stolen with the purpose of using their financial resources or to take a loan or credit card in their name then such a crime is known as Identity theft.
- **Cyberterrorism -** When a threat of extortion or any kind of harm is being subjected towards a person, organization, group or state, it is known as the crime of Cyber Terrorism. Generally, it includes the well-planned attack strategies on the Government and corporate computer system.
- **Cyberbullying -** When a teenager or adolescent harasses, defames, or intimidates someone with the use of the internet, phone,

* The views expressed are personal views of the author and it should not be taken as views of the NIRC-ICSI

chat rooms, instant messaging or any other social network then the person is said to be committing the crime of Cyberbullying. When the same crime is done by adults it is known as Cyberstalking.

- Hacking - The most common cybercrime is Hacking. In this crime, the person gets access to other people's computers and passwords to use it for their own wrongful gain.
- Copyright - With the massive surge in internet users, when the data/ information is distributed on all platforms, copyrighting your work aids you to restrict the use of your work. Any use of your copyrighted without your permission is a punishable offence.
- Trade Secrets - Internet organization spends a lot of their time and money in developing softwares, applications, and tools and rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offence.
- Harassment and Stalking - Harassment and stalking are prohibited over internet platforms as well. Cyber laws protect the victims and prosecute the offender against this offence.

Objectives of Cyber Laws (Information Technology Act, 2000):

- To provide legal recognition for all e-transactions
- To give legal recognition to digital signatures as a valid signature to accept agreements online
- To give legal recognition to keeping accounting books in electronic form by bankers as well as other organizations
- Protection of online privacy and stopping cyber crimes
- To build capabilities to prevent and respond to cyber threats.
- To safeguard information and information infrastructure in cyberspace.

Advantages of Cyber Laws

Cyber law is extremely important for organizations that are vulnerable because of their ineffective cyber security system.

- Secured E-Commerce Infrastructure for online businesses.
- Digitally sign your contracts/ papers
- Introduced new businesses for Certifying Authorities
- Proficient use of E-Forms as prescribed
- Secured websites with Digital Certificates
- Meticulous monitoring on the web traffics
- Electronic Transactions safeguarded
- Emails are a legal form of communication and are approved in the court of law.

Compliance Audit under Cyber Laws:

In this present global era, Audits are not only associated with verification of any financial transaction. Now the meaning of audit has been expanded to include corporate law, cyber law , and other legal compliances of the company. The cyber compliance audit is the first step in protecting sensitive and confidential information as it includes a thorough analysis of e-contracts document and other company data.

Types of Audit	Reasons for Audits
1. Mobile Application Security Audit	Mobile phones are increasingly used to surf the Internet, store private information, access corporate network /confidential company information. With lots of features smart phones now have become an attractive target for Malware, Phishing attacks and much more specially crafted cyber attacks.
2. Web Application Security Audit	Web App Security audit helps the enterprises to improve their security at every level of the life cycle i.e. in the design phase, implementation phase or even when the software is running in the production environment.

3. Network Security Audit	Network Security audit is categorized into two vital areas of information. The first area is the static data which would cover the system definitions, protocols used to communicate, password rules, firewall definitions etc. whereas the second category looks into the activities, events that have taken place which would cover areas such as database access, file transfers, sharing, system log on etc. are some of the times that will be looked into the network audit.

How to prevent Cyber Crime?

As we all know that "prevention is always better than cure". Though cyber laws in India provide protection from cybercrime and legal aid but still we can take preventive measures to defeat cyber crimes. Some of them are given below:

- **Using of Anti-virus:** trusted not free downloaded / pirated.
- **Use strong passwords:** Don't repeat your passwords on different sites, and change your passwords regularly. Make them complex. A password management application can help you to keep your passwords locked down.
- **Keep your software updated:** This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits or flaws in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.
- **Downloads on the mobile phone -** Download everything on the mobile phone from a trustworthy source only.

- **Rating and feedback -** Always check for the seller's rating and feedback of customers for the seller. Be sure that you are checking current feedbacks. Also, beware of feedbacks that are 100% seller favoring or have an entry on the same date.
- **Personal Information Request -** Everyone must have received a call or mail. In which, the person on the other side asks for personal information. This includes your card CVV or a mail containing an attachment which requires you to click on embedded links. Be sure to never respond to such emails or calls.
- **Keep up to date on major security breaches:** If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.
- **Be Social-Media Savvy:** Make sure your social networking profiles (e.g. Facebook, Twitter, YouTube, MSN, etc.) are set to private. Be careful what information you post online. Once it is on the Internet, it is there forever!
- **Secure your wireless network:** Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Avoid conducting financial or corporate transactions on Public networks.

Cyber security assessment framework

Cyber Security Framework has been adopted for use across a wide variety of industries because of its comprehensive nature and sound guidance. It is much needed things for the Corporate to conduct an assessment and the same will vary with organizational size, complexity, and industry type. This will help to address immediate and future security priorities.

The framework addresses five important aspects of cyber security including: identify, detect, protect, respond, and recover.

Cyber security assessment framework in Brief

1. Involve people with the necessary experience and skills along with appropriate depth of technical skills and knowledge of the current risk environment.
2. Evaluate the full cybersecurity framework rather than cherry pick items.
3. Understand the current state against framework characteristics, where the organization is going, and the minimum expected cybersecurity practices across the industry or business sector.
4. It is not intended to be an exhaustive analysis requiring extensive testing. Rather, the initial assessment should drive additional risk-based cyber security deep dive reviews.

Conclusion:

In the present world which is more tech-savvy, the words cyber law and cyber crimes have also become more sophisticated. As the nature of the internet is anonymous, it is easy to commit cybercrimes. Therefore, the Information Technology Act, 2000 or also known as the Indian Cyber Act or the Internet Law came to force in India. It is important for anyone using the internet to be aware of the cyber laws to avoid penalty or punishment under these laws. Strict cyber laws are the need of this global era where technology is growing at rapid speed. ■

Forensic Audit- "BRAHMASTRA" to combat Corporate Wrongdoing

CS Shweta Jain, ACS
shweta.jain2003@gmail.com

The five E's being 'Effective, Efficient, Easy, Empower, and Equity', the pillars of corporate governance demands transparent and globally viable approach but concurrently paves way for fraud, scams, financial misrepresentation, etc.

Forensic Audit is such an investigation tool that allows minute & detailed investigation into the financial records to an extent which could be used in the legal proceedings or presented before the court of law, to battle Fraud and Embezzlement took place in the Corporate. The evidentiary nature constitutes Forensic Audit as a never-to-be-dimmed tool-mix for accounting, auditing and legal investigation.

A forensic audit is factually the **analysis and investigation** of the financial records, corporate affairs, key personal of any corporate to extract out the facts and information which can be suitably used in the court of law. It is the specialized stream of Audit which requires expertise in Accounting, Auditing and legal framework to enable large spectrum of investigation. The essence of Forensic Audit lies with the fact that it provides a clear understanding of the financial position along with the connection of the communications related to that.

Motive & Object:

There are numerous reasons causing Forensic Audit a must in the corporate world; as a glimpse the following can be presented herein below:

1. Corruption
2. Asset Misappropriation
3. Financial Statement Fraud
4. Conflict of Interests
5. Extortion

Broadly, FRAUD FINDING is the real and actual motive behind conducting Forensic Audit and Forensic Auditors dig deep into that direction which covers areas such as:

a. Fraud Finding
b. Fraud detection and prevention techniques
c. Auditing attributed to Fraud
d. Investigation and analysis of financial evidence
e. Development of specialized computerized applications as per corporate activities and industry
f. Preparation and Presentation of facts & findings in the form of reports, documents, etc.

Fraud Finding as the basic intention behind Forensic Audit, but what is Fraud???

As per Business Dictionary, 'Fraud' is an act or course of deception, an intentional concealment, omission, or perversion of truth, to:

(1) Gain unlawful or unfair advantage
(2) Induce another to part with some valuable item or surrender a legal right, or
(3) Inflict injury in some manner

Moreover, **'Willful fraud' is a criminal offence** which calls for severe penalties and its prosecution and punishment (like that of a murder) is not bound by the statute of limitation.

Key Benefits of Forensic Audit can be summarized with the formulae of PRP –

- Prevention
- Regulation
- Penalisation; of Financial Frauds and Scams

In the emerging New India Movement where good corporate governance is in focus and practice of Social, Economic & Political Equity is emphasized majorly by all the initiatives of Government of India, regulatory authorities and departments like Enforcement Directorate (ED) and the Serious Fraud Investigation Office (SFIO) have also emphasized the need for forensic audit following the rise in

* The views expressed are personal views of the author and it should not be taken as views of the NIRC-ICSI

money laundering and Willful default cases that are plaguing the banking system, to nourish the economy in a better way by providing financial stability.

As per New India Movement, 2022 the modern phase of making a India as free from corruption, Scam & Fraud on the lines of good governance, Forensic auditing is a –

- Rapidly growing area as a specialized branch of accounting and investigations and
- Is concerned with the detection and prevention of financial fraud and white-collar criminal activities.

Presently we are witnessing a plethora of Government initiatives including Ease of Doing Business, Start-Up India, Stand Up India, Digital India along with reformative regulating regime with the implementation of GST, Direct Tax Code, Insolvency and Bankruptcy Code, RERA, Companies Amendment Acts, Forensic Audit, Class Action Suit, Valuation etc. All such initiatives can be successful and fruitful only if the termite presented in the form of Fraud and Corruption is eliminated from the corporate lifeline because otherwise it will keep on hampering the growth, prosperity and success of corporate and ultimately the Economy.

Forensic Audit in such a scenario is an effective tool-mix because it carries a detailed analysis & investigation of minute financial transaction, record, document, statement etc with a motive to present as an evident in the House of Law and that is the beauty of Forensic Audit.

Forensic Auditors are the experts not only in Accounting, Auditing but in legal framework and having their expertise in finding criminal trail paves the way for fraud detection and diagnosis.

Cyber Forensic

Certainly, the advancement of IT and Communication has led to the emergence of a new kind of crime called the Cyber Crime. It is the crime wherein, the computer or the data itself is either a target or the object of an offence or a tool employed in committing some offence, and thus providing the necessary inputs for that offence.

Cyber-crimes are technology-based crimes wherein the computer or internet itself is used as a weapon or means to commit such crimes. They are organized and white-collar crimes like cyber frauds, hacking, data theft, phishing, identity theft, etc. are committed with the help of technology and cyber criminals have a deep understanding of technology. In fact, cyber criminals are technocrats who understand the intricacies of Information Technology. Cyber- crimes are beyond any territorial or geographical boundary or barrier.

Generally, a Cyber Crime can be classified into the following three categories:

1. **Target Cyber Crime:** It is a crime wherein a computer is the target of the offence.
2. **Tool Cyber Crime:** It is a crime wherein a computer is used as a tool in committing the offence.
3. **Computer incidental:** It is a crime wherein the computer plays only a minor role in the commission of the offence. ■

Forensic Audit- Thorough View

CS Parmeet Kaur Lottey, ACS
parmeetkaur579@gmail.com

FORENSIC AUDIT – MEANING

The term 'forensic audit' has not been defined under any statue, therefore for the meaning of the same, reliance has been placed on dictionary meaning.

In general, Forensic Audit represents an area of finance that combines detective skills and financial acuity.

Forensic audit also known as forensic accounting is an examination of evidence regarding an assertion to determine its correspondence to established criteria carried out in a manner suitable to the court.

Investopedia

Forensic Audit is an examination and evaluation of a firm's or individual's financial information for use as evidence in court. A Forensic Audit can be conducted in order to prosecute a party for fraud, embezzlement or other financial claims. In addition, an audit may be conducted to determine negligence or even to determine how much spousal or child support an individual will have to pay.

Collin Greenland (2001), Demystifying Forensic Accounting, the Weekend Observer, Pg. 5, December 7, 2001

Forensic accounting (or auditing) is the integration of accounting, auditing and investigative skills in order to provide an accounting analysis suitable for the resolution of disputes (usually but not exclusively) in the courts.

Jack Bologna and Robert J. Lindquist (1987), Fraud Auditing and Forensic Accounting : New Tools and Techniques, by, JohnWiley & Sons, New York

Forensic Audit as the application of financial skills and an investigative mentality to unresolved issues, conducted within the context of the rules of evidence. As a discipline, it encompasses financial expertise, fraud knowledge, and a strong knowledge and understanding of business reality and the working of the legal system.

NEED OF FORENSIC AUDIT

With the increase in the financial frauds popularly known as white collar crimes, forensic auditing and accounting have risen to prominence for ensuring the directed growth of the corporates and inclusive growth of economy.

In the contemporary times, when the Government is looking forward for a robust economy and nation building at par, financial stability is a must in the corporate. Henceforth, Forensic audit submits various recompenses in ensuring commercial health of the companies through aiding in the Prevention, Regulation and Penalization of financial frauds and scams.

In the previous years too, India has witnessed financial frauds which affected the golden growth of India's economy. The Investigations and risk consulting firm Kroll unearthed in their survey23 that 69% of companies studied were affected by fraud in Financial Year of 2013, up from 68% in the previous year. The value of fraud, the study found, rose to 71% from 67%. Insider fraud was particularly rife in India, with 89% of respondents indicating the perpetrator was an insider of some sort — a junior, middle management or senior employee, or an agent.

Indeed, the recent upswing in the financial frauds in India, compelling more management to conduct forensic audits in the interest of our growing economy.

Further, provisions of the Companies Act mean that every company now has to have proactive fraud risk management policies. The Act requires independent directors to increase safeguards against fraud and reminds them of their

* The views expressed are personal views of the author and it should not be taken as views of the NIRC-ICSI

whistleblowing responsibilities.

The Enforcement Directorate and the Serious Fraud Investigation Office have also emphasized the need for forensic audit following the rise in money laundering and Willful default cases that are plaguing the banking system.

The above discussion confirms that in order to assist in the paramount growth of Indian economy on the global platform under the realm of good governance, transparency, accountability and uprightness, Forensic Audit has become a need of the hour.

WHY FORENSIC AUDIT IS IMPERATIVE?

Forensic Audit is a strategic approach in detecting the financial frauds in the organizations along with enhancing their financial stability at par. In this context, benefits of Forensic Audit are listed below:

1. **Detection and Responsibility of Corruption:** It aids in detecting the corruption in the corporates and also determines responsibility of the person liable for the corruption and its practices.
2. **Detection of Asset Misappropriation:** This is the most common and prevalent form of fraud. Misappropriation of cash, raising fake invoices, payments made to non-existing suppliers or employees, misuse of assets, or theft of Inventory are a few examples.
3. **Detection of Financial Statement Fraud:** This type of fraud tries to show the company's financial performance as better than what it actually is. The goal is to improve liquidity, ensure top management continues receiving bonuses, or to deal with pressure for market performance. Some examples are, intentional forgery of accounting records, omitting transactions – either revenue or expenses, non-disclosure of relevant details from the financial statements, or not applying the requisite financial reporting standards.
4. **Fraud Identification and Prevention:** Fraud is quite common in big organizations where the number of daily financial transactions is huge. In such an environment, an employee can easily undertake fraudulent activities without being caught. Forensic accounting helps in analyzing whether the company's accounting policies are followed or not, and whether all the transactions are clearly stated in the books of accounts. Any deviation observed in the books of accounts can help in identifying fraud, and necessary measures can be taken to prevent it in the future.
5. **Making Sound Investment Decisions:** It provides a path for investors to make thoughtful investment decisions. Further, many organizations also apply for loans from various financial institutions. By performing an analysis, such institutions can come to a decision on whether they would like to fund a company or not.
6. **Formulation of Economic Policies:** Various cases of fraud that becomes evident after forensic analysis act as a reference for the government to formulate improved economic policies that would be able to curb such fraudulent activities in the future. So, the government can strengthen the economy and prevent such illegal activities in the country.
7. **Rewarding Career Opportunity:** As a career, forensic auditing is extremely rewarding, as it not only involves regular auditing and accounting activities, but also involves identification, analysis, and reporting of the findings during an audit. The acceptance of reports generated by a forensic auditors by the court of law gives them an upper hand as compared to other accountants.

TYPES OF FRAUDS

Fraud in legal parlance could be categorized in two categories, which includes:

1. **Fraud as a Civil Wrong,** is a tort. While the precise definitions and requirements of proof vary among jurisdictions, the requisite elements of fraud as a tort generally are the intentional misrepresentation or concealment of an important fact upon which the victim is meant to rely, and in fact does rely, to the harm of the victim. Victim to prove fraud by clear and convincing evidence.
2. **Fraud as a Criminal offence,** takes many different forms, some general (e.g., theft by false pretense) and some specific to particular categories of victims or misconduct (e.g., bank fraud, insurance fraud, forgery). The

elements of fraud as a crime similarly vary. The requisite elements of perhaps the most general form of criminal fraud, theft by false pretense, are the intentional deception of a victim by false representation or pretense with the intent of persuading the victim to part with property and with the victim parting with property in reliance on the representation or pretense and with the perpetrator intending to keep the property from the victim.

Kinds of Fraud in specific to Economy and Financial Transactions

In specific to the impact on economy and financial transactions, frauds could be categorized as below:

1) Bank frauds
2) Corporate frauds
3) Insurance frauds
4) Cyber frauds
5) Securities frauds

1. **Bank Frauds:** Bank fraud is a big business in today's world. The number of bank frauds in India is substantial. It is in increasing with the passage of time in all the major operational areas in banking. There is different area in Bank Deposits, loan, inter branch, accounting, transaction, etc.
2. **Corporate Frauds:** In India, Corporate Frauds from leading Indian business are shaking the economy time and again. From Satyam Computers stunned the national financial world in 2009, when Satyam's Founder B. Ramalingan Raju declared he had inflated profit and jacked up the company's Balance Sheet by more than one billion dollars to the recent incident of PNB Fraud in year 2017, Frauds are apparent in the corporates. This needs to be checked strictly to ensure financial stability and emerging economy.
3. **Insurance Frauds:** There are different types of frauds in insurance sectors.
   E.g. health insurance, claims fraud, false claims, insurance speculations, application frauds, etc.
4. **Cyber Frauds:** Cyber Frauds are the frauds done with the help of the internet targeting the unauthorized use of digital instruments like credit card, ATM card, cyber equipment's at home etc.
5. **Securities Frauds:** Apart from Corporate Frauds, Frauds in the Securities and Securities Market are also affecting many people time and again. From the perspective of frauds in securities, investor community could not forget the under truncate Rs. 4000 crore of Harshad Metha scam and over Rs. 1000 Crore of Ketan Parekh scams which duped the shareholder with the loss of their wealth in the big markets. In addition to this, the instances of Insider trading are also considered securities fraud in many circumstances.

LIVE CASES

Forensic Audit on PNB Scam:

Punjab National Bank conducted forensic audit of jeweller Nirav Modi's companies, according to people directly briefed on the matter.

The bank issued a formal appointment letter to the Belgium-headquartered audit firm on February 27, 2018 to conduct a forensic audit in the scam wherein Modi, his uncle Mehul Choksi and their companies have been accused of defrauding the bank of as much as Rs 12,700 crore.

In the starting of January, 2018, PNB informed the BSE (Bombay Stock Exchange) that it has detected some "fraudulent and unauthorized transactions" in one of its branches in Mumbai to the tune of $ 1771.69 million (approx.). Following the announcement, the share price of the state-owned bank plunged 10%.

Meanwhile, the Central Bureau of Investigation (CBI) received two complaints from PNB against billionaire diamantaire Nirav Modi and Jewellery Company alleging fraudulent transactions worth about Rs. 11, 400 crores, the Press Trust of India reported. This is in addition to the Rs. 280 crore fraud case that he is already under investigation for, again filed by PNB.

Forensic Audit on Dena Bank:

The Finance Ministry ordered forensic audit of Dena Bank and Oriental Bank of Commerce after some of their Mumbai-based branches allegedly misappropriated funds worth Rs. 437 crores, mobilised through fixed deposits. Professional services firm KPMG in India has been given the mandate to undertake forensic investigations. In the case of Dena Bank, the misappropriation was to the tune of Rs. 257

crore and related to funds mobilised from seven corporate. In Oriental Bank's case, it related to misappropriation of funds amounting to Rs. 180 crore, reportedly belonging to the Jawaharlal Nehru Port Trust. The Central Bureau of Investigation is already looking into the alleged fraud. The developments are disparate ones and took place at different times. The incidents have again brought to the fore the weak risk management systems in public sector banks.

DIFFERENCE BETWEEN AUDIT AND FORENSIC AUD

Basis	Audit	Forensic Audit
Objective	To express opinion as to 'true & fair' presentation	To determine correctness of the accounts or whether any fraud has actually taken place
Audit Period	Generally, all transactions for the particular accounting period are covered	Forensic audits don't face any such limitations. It may be conducted any number of financial year or part of financial year.
Reliance	For ascertaining the accuracy of the current assets and the liabilities auditor relies on the management certificate or representation of management.	Forensic auditors are required to carry out the independent verification of suspected or selected items.
Techniques used	Techniques used are more of 'Substantive' and 'compliance' procedures.	Techniques used are analysis of past trend and substantive or 'in depth' checking of selected transactions.
Quantification	In case of the adverse findings, the auditor expresses the qualified opinion, with/without quantification.	In case of the adverse findings, the forensic auditors are required to quantify.

ROLE OF COMPANY SECRETARY

It is reiterated time and again that Good Governance is paramount for the inclusive growth of the country while promoting the community confidence, their participation, transparency, accountability, lead for the better decisions embarking the welfare of the masses and supporting the ethical decision making, which all in consolidation call for the emergent and bright future of the nation at global platform. In the similar context, India has opted to Reform, Perform, Transform under vision New India, 2022, adhering to the best practices of good governance. In this direction, we are witnessing various legal reforms like GST, RERA, IBC, and initiation of amendments in Prevention of Money-laundering Act, 2002 through Finance Act, 2018 and alike.

When talking the all compassing growth, economic growth is one of the significant spheres to be adhered with the premium practices of good governance and henceforth the glitches bugging the emerging growth of economy are tackled by the government at priority.

In this context among other things, Corporate Frauds are considered as one of the major challenges which is obstructing the growth of corporates as well as of economy as a whole.

The role of company secretaries is expanding in the era of forensic audit wherein they are crucially assisting in preventing, regulating and penalizing the instance of corporate frauds. Right from conducting forensic audit to examining the evidences, from finding the culprit behind the fraud to appearing in the court for submitted the testimony, a Company Secretary is apt in serving his professional excellence as a forensic auditor.

To summarize, where forensic audit is a detailed engagement which requires the expertise of not only accounting and auditing procedures but also expert knowledge regarding the legal framework and a forensic auditor is required to have an understanding of various frauds that can be carried out and of how evidence needs to be collected.

In this context, Company Secretary is a Catalyst in Upholding Good Governance via Forensic Audit. His role in specific to Forensic audit is discussed as below.

PROCEDURE

A forensic auditor is required to have special training in forensic audit techniques and in the legalities of accounting issues. A forensic audit has additional steps that need to be performed in addition to regular audit procedures. Forensic Audit could be done with the adoption of the procedure detailed as below:

Step 1 – Accepting the Investigation

A forensic audit is always assigned to an independent firm/group of investigators in order to conduct an unbiased and truthful audit and investigation. Thus, when such a firm receives an invitation to conduct an audit, their first step is to determine whether or not they have the necessary tools, skills and expertise to go forward with such an investigation. They need to do an assessment of their own training and knowledge of fraud detection and legal framework. Only when they are satisfied with such considerations, can they go ahead and accept the investigation.

Step 2 – Planning the Investigation

Planning the investigation is the key step in a forensic audit. The auditor(s) must carefully ascertain the goal of the audit so being conducted, and to carefully determine the procedure to achieve it, through the use of effective tools and techniques. Before planning the investigation, they should be clear on the final categories of the report, which are as follows:

- Identifying the type of fraud that has been operating, how long it has been operating for, and how the fraud has been concealed.
- Identifying the fraudster(s) involved.
- Quantifying the financial loss suffered by the client.
- Gathering evidence to be used in court proceedings.
- Providing advice to prevent the recurrence of the fraud.

Fraud Triangle and Fraud Risk

A fraud triangle is a tool used in forensic auditing that explains three interrelated elements that assist the commission of fraud- Pressure (motive), opportunity (ability to carry out the fraud) and rationalization (justification of dishonest intentions). Fraud risk is the vulnerability, a company/organization has towards those who are capable of overcoming the three elements in the fraud triangle. Fraud risk assessment is the identification of fraud risks that exist in the company/organization. The planning involves the formulation of techniques and procedures that align with the fraud risk and fraud risk management.

Planning also includes the identification of the best way/mode to gather evidence. Thus, it is necessary that ample research is done regarding certain investigative, analytical, and technology-based techniques and also related legal process, with regard to the outcome of such investigation.

Step 3 – Gathering Evidence

In forensic auditing specific procedures are carried out in order to produce evidence. Audit techniques and procedures are used to identify and to gather evidence to prove, for example, how long have fraudulent activities existed and carried out in the organization, and how it was conducted and concealed by the perpetrators. In order to continue, it is pertinent that the planning stage has been thoroughly understood by the investigating team, who are skilled in collecting the necessary evidence. Techniques such as computer-assisted audit techniques, discussions and interviews with employees, reconciliations, cash counts and reviews of documentation, forensic data analysis, electronic and physical surveillance etc. can be used.

Step 4 – Reporting

The reporting stage is the most obvious element in a forensic audit. After investigating and gathering evidence, the investigating team is expected to give a report of the findings of the investigation, and also the summary of the evidence and conclusion about the loss suffered due to the fraud. It should also include the plan of the fraud itself, and how it unfolded, basically the whole trail of events, and suggestions to prevent such fraud in the future.

Step 5 – Court Proceedings

The last stage expands over those audits that lead to legal proceedings. Here the auditors will

give litigation support as mentioned above. The auditors are called to Court, and also included in the advocacy process. The understanding here is that they are called in because of their skill and expertise in commercial issues and their legal process. It is important that they lay down the facts and findings in an understandable and objective manner for everyone to comprehend so that the desired action can be taken up. They need to simplify the complex accounting processes and issues for others to understand the evidence and its implications

RED FLAGS

- ✓ Red flags are nothing but symptoms or indicator of situation of fraud.
- ✓ A red flag is a set of circumstances that are unusual in nature or vary from the normal activity.
- ✓ It is a signal that something is out of the ordinary and may need to be investigated further.

Note: Red Flags aid the Auditor's Responsibility to Consider Fraud & Error. It is effective for all audits relating to accounting periods commencing on or after 1st April 2009.

Common Types of Red flags

The most common types of Red Flags and fraudulent activity can be categorized as:

1. **Employee Red Flags are like,** employee lifestyle changes, expensive cars, jewellery, homes, Significant personal debt and credit problems, behavioral changes (these may be an indication of drugs, alcohol, gambling)
2. **Management Red Flags are like,** reluctance to provide information to auditors,

Managers engage in frequent disputes with auditors, Management decisions are dominated by an individual or small group, Managers display significant disrespect for regulatory bodies, weak internal control environment, Accounting personnel are lax or inexperienced in their duties, Significant downsizing in a healthy market Continuous rollover of loans, Unexpected overdrafts or declines in cash balances Frequent changes in banking accounts, Frequent changes in external auditors etc.

GREEN FLAGS

Above discussion on Red Flags says that red flags are symptoms or indicators of fraud, white collar crime or something detrimental to the interest of the organization. To the contrary there are other signals which could also imply the existence of fraud but do not activate alarm bells. Rather they may even lead to a greater sense of assurance and comfort in a scenario which may be potentially infused with fraud. These signals are referred as 'green flags'.

The instance of Green Flags could be helpful in identifying are unusual signs or inconsistencies, but apparently harmless or perhaps even helpful.

LEGAL FRAMEWORK

The position of Laws and Regulations dealing with Corporate Fraud and also aids in achieving forensic audit would be discussed under the following heads:

1. Companies Act, 2013
2. Indian Penal Code
3. Prevention of Corruption Act, 1988
4. Information and Technology Act, 2000
5. SEBI Act, 1992
6. ICSI Anti Bribery Code.

CASE LAWS

Sahara Group Scam

Sahara Group chairman Subrata Roy and Vijay Mallya had a lot in common. Both successful businessmen had a passion for sports. The two also had their own IPL teams, Sahara Pune Warriors and Royal Challengers Bangalore (after resigning as the chief of UB Group Mallya is technically not the owner of RCB). In fact, the duo jointly owns the Sahara Force India Formula one team.

Sahara Group was accused of failing to refund over Rs. 20,000 crores to its more than 30 million small investors which it collected through two unlisted companies of Sahara.

In 2011, SEBI ordered Sahara to refund this amount with interest to the investors, as the issue was not in compliance with the requirements applicable to the public offerings of securities.

Roy was arrested on 28th February 2014 and remained behind bars as an under- trial. His proposal to settlement of the matter was rejected by the court and SEBI.

Satyam Computers

B Ramalinga Raju, the founder of Satyam Computers, got into trouble after he admitted

to inflating the company revenue, profit and profit margins for every single quarter over a period of 5 years, from 2003-2008. The amount misappropriated in this case is estimated to be around Rs. 7,200 crore.

In April 2015, Ramalinga Raju and his brothers were sentenced to 7 years in jail, and fined Rs. 5.5 crore.

Some governance problems, which have been noticed in the collapse of Satyam are unethical conduct, avoiding tax payment, false books and bogus accounting, Unconvinced role of independent Directors, Questionable role of Audit Committee, Dubious Role of Rating Agencies, Fake Audit.

Saradha Chit Fund

Saradha group which ran a chit fund in West Bengal had collected around ₹200 to 300 billion from investors with a promise of high returns for their investments.

The company which enjoyed strong political backings collapsed in April 2013. The amount investors lost is estimated to be between Rs. 2060 – 2400 crores.

Ketan Parekh Scam

Parekh was involved in circular trading and stock manipulation through 1999- 2001 in a host of companies. He borrowed from banks like Global Trust Bank and Madhavpura Mercantile Co-operative bank, and manipulated a host of stocks popularly known as K-10 stocks.

Among others, PNB and Satyam are clear audit failures. In Satyam direct confirmation from bank was not sought despite the materiality of the same. In PNB, Swift messages serial number wise should have traced to the transaction entry in the general ledger at least on test check basis and the scam would have come to light automatically much earlier. ■

THE INSTITUTE OF Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

NORTHERN INDIA REGIONAL COUNCIL

INITIATIVES OF CHAPTERS

AGRA

Agra Chapter has organized two Webinar on theme "Responsibility of Professionals in Nation Building" on 7th November 2020 and "NBFCs-A Beginning Towards Self Reliant India" on 28th November 2020. Agra Chapter has also organized the 19th All India Debate Chapter Level Competition for the Students of the ICSI on 4th December 2020.

AJMER

Ajmer Chapter organised a webinar on theme "Step Ahead for NBFCs" on 13th November 2020. Ajmer Chapter also organised a webinar on theme "Consumer Protection Act, 2019" on 23rd November 2020. The Chief guest was CS Manish Gupta, Council Member of ICSI.

BHILWARA

Bhilwara Chapter organised webinar on the topic "LODR- General Complience" on 21st November, 2020. The Chief Guest of Programme was Shri U. S. Patole, ROC-cum-OI, Jaipur and the Special guest of the webinar was CS Ranjeet Pandey, Immediate Past President, ICSI.

CHANDIGARH

Chandigarh Chapter has conducted its 7th Webinar on "Amendments in Companies Act,2013" in which CS Suresh Pandey, Chairman, NIRC of ICSI was Special Guest.

Chandigarh Chapter organized "Students' Conference" through online mode. The theme of the same was "Professionalism at the behest of CS Profession". CS Ashish Garg, President, ICSI was the Guest of Honour.

FARIDABAD

1. CS Executive Mod-1 Batch postponed and started again 6th November, 2020
2. CSEET 2nd Batch Mock Test series held on 15th to 20th November for students appearing 21st Nov,2020 Exam
3. Two addl Examination Centre search and finalise for conducting CS Dec,2020 Exam.. As of Now, Fbd Chapter is having 4 Examination Centre for Dec,2020 CS Exam.
4. Completion work of Solar Panel of the roof of the Chapter building.

GHAZIABAD

1. Ghaziabad Chapter organized Moot Court Competition through online mode on November 26, 2020 and send the details of the winners to NIRC for the Regional Level.
2. Ghaziabad Chapter of NIRC of ICSI organized a Webinar on the theme "Latest Amendments in GST" on Tuesday, November 10, 2020.

3. Ghaziabad Chapter of NIRC of ICSI organized a Webinar on "ICSI Auditing Standards" on Saturday, November 21, 2020. .
4. Ghaziabad Chapter released its 18th Monthly Newsletter for members and students and also invited Articles and Write-ups for our Chapters forthcoming monthly e-Newsletter.
5. We have running successfully our OT Classes by Online Mode.

GORAKHPUR

Gorakhpur Chapter conducted a webinar on the topic "Important Aspects of Merger and Amalgamation" on 24th October 2020. The Chief Guest of the programme was Shri Satish Dwivedi, Hon'ble Minister of State (Independent Charge), Basic Education, Uttar Pradesh. The Guest of Honour was CS Suresh Pandey, Chairman, NIRC of ICSI and the Special Guest was CS Amit Gupta, Regional Council Member, NIRC of ICSI.

Gorakhpur Chapter organised a webinar on the theme Economic Revival through Capital Markets post COVID-19 on 01st November 2020 to celebrate Capital Market Week.

Gorakhpur Chapter has entered into a tie-up with four (4) leading hospitals of Gorakhpur - Hope Panacea Super Speciality Hospital, Radiant Healthcare Hospital, Mansi Hospital and Jeevandayini Medical and Eye Healthcare Centre, for discounted services for our members, students, employees and their dependents.

Gorakhpur Chapter also conducted 03 Career Awareness Programmes on 06th November 2020 in Sardar Ballabh Bhai Patel Girls Inter College, Sardar Ballabh Bhai Patel Boys Inter College and Chandra Patel Inter College in which more than 300 students and faculties participated.

The ICSI signed a MoU with Siddharth University (State University), Kapilvastu, Sidhharth Nagar, Uttar Pradesh on 09th November 2020 in which Siddharth University has signed the MoU for providing necessary recognition to Company Secretary qualification as equivalent to Post Graduate Degree for the pursue of admission to Ph.D. in Siddharth University and for ICSI Signature Award.

GURUGRAM

1. Webinar on Auditing Standards Issued by ICSI on 23.10.2020
2. Webinar on FCR Amendment Act, 2020: Role of CS on 30.10.2020
3. Webinar on Opportunities in Job as well as in Practice for CS in Insurance Sector as Compliance Professionals on 21.11.2020
4. Webinar on RERA – How to Proceed Complaints and Appeals – Role of CS on 28.11.2020
5. Webinar on How to Attract PE/VCs for funding in startups on 30.11.2020
6. Online Career Awareness Program in Jain Girls Sr. Sec. School, Rewari on 19.11.2020
7. Online Career Awareness Program in Ansal University, Gurugram on 24.11.2020

JAIPUR

Jaipur Chapter has organised 3 webinars in the month of Nov, 2020. we have also published Nov 2020 issue of "Jaipur Chapter's E-Newsletter".

JODHPUR

Jodhpur Chapter organised a Career Awareness Program at Aurobindo Centre of New Education. The Chapter also organised Webinar on Issue, Transfer and Reporting of Equity Instruments under FDI.

Initiatives of Chapters of NIRC of ICSI

KANPUR

Kanpur Chapter of NIRC of ICSI organised a Webinar on the Topic "The Latest Companies Amendments (Act) 2020" on 11th November, 2020. CS Nagendra D. Rao, Vice-President of ICSI was the Special Guest.

Kanpur Chapter of NIRC of ICSI also organised a Webinar on the Topic "Loan Syndication" on 27th November,2020.

KOTA

Kota chapter visited Bundi district for the establishment of Study centre.

NOIDA

Two Webinars have been conducted in November 2020 with maximum participation from Members.

PANIPAT

Panipat Chapter signed MOU for Academic Collaboration with ICSI and Om Sterling Global University, Hisar, Haryana Examination Center has been established at Rohtak and Bhiwani.

Panipat Chapter organised webinar on 04th Nov, 2020 on the topic "ICSI Auditing Standards". The Chief Guest was CS Manish Gupta, Central Council Member , The ICSI and the Special Guest- CS Monika Kohli, Regional Council Member NIRC - ICSI.

Panipat Chapter also organised a webinar on 23th Nov, 2020 on "PROFESSIONAL OPPORTUNITIES UNDER FOREIGN CONTRIBUTION REGULATION ACT, 2010 (FCRA)"

The Chief Guest was CS Ranjeet pandey, Immediate Past President, The ICSI and the Special Guest was CS Amit Gupta, Regional Council Member NIRC-ICSI.

PRAYAGRAJ

Prayagraj Chapter organised 02 Webinar; The 1st on 11.11.2020 on Topic "EPF & ESI Compliances- Opportunities for Company Secretaries".

The 2nd one on 28.11.2020 on Topic: "Recent Amendments and Practical aspects of Income Tax Returns".

UDAIPUR

1. On 25th November, 2020 -1st Academic Collaboration was done between ICSI and Janardan Rai Nagar Rajasthan Vidyapeeth University at Udaipur. CS Suresh Pandey , Chairman of NIRC of ICSI was the authorised signatory on behalf of the institute ICSI and Prof. (Col.) S.S. Sarangdevot Vice-Chancellor of Janardan Rai Nagar Rajasthan Vidyapeeth University was the authorised signatory on behaf of the Janardan Rai Nagar Rajasthan Vidyapeeth University. CS Ashish Garg President, ICSI and CS Nagendra D. Rao Vice-President, ICSI also present virtually on MOU Signing Programme.
2. On 25th November, 2020 -2nd Academic Collaboration was done between ICSI and Pacific University at Udaipur. CS Suresh Pandey , Chairman of NIRC of ICSI was the authorised signatory on behalf of the institute ICSI and Prof. K.K. Dave President of Pacific University was the authorised signatory on behaf of the Pacific University. CS Ashish Garg President, ICSI and CS Nagendra D. Rao Vice-President, ICSI also present virtually on MOU Signing Programme.
3. Chapter Conducted Online Career Awarness Programme for Students.

THE INSTITUTE OF
Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

10 CPE Credits for Members (under structured category) 20 PDP Hours for Students

48th National Convention of Company Secretaries

Theme : Governance: From Grassroots to Global

Dear Professional Colleague,

The **48th National Convention of Company Secretaries** is scheduled to be held at Amber Convention Centre, Indore, Madhya Pradesh on December 17-18-19, 2020 (Thursday-Friday- Saturday) on the theme **"Governance: From Grassroots to Global"**.

Coverage

- **Atmanirbhar Bharat: Parliamentary Discipline in building self reliant India**
- **Rewriting the Rules of Good Governance**
- **Building Smarter Workforces: The altering dynamics and needs of India Inc.**
- **Learning Governance from Ancient Indian Scriptures**
- **Panchayat Governance: Elevating good governance standards for the masses**

Speakers

Eminent speakers and experts with comprehensive exposure on the practical aspects of the topics will address and interact with the participants.

Delegate Registration Fee* (non-residential)

Delegate Category	Early Bird payment upto November 12, 2020	Early Bird payment upto December 10, 2020	Payment December 11, 2020 onwards
Members	INR 6500	INR 8000	INR 8500
Practicing Company Secretaries	INR 6000	INR 7500	INR 8000

*Only 200 seats on First Come First Serve basis as per MHA Guidelines
GST @ 18% applicable on above fee

Delegate Registration Fee* (for attending on virtual platform)

Delegate Category	Early Bird payment upto November 12, 2020	Early Bird payment upto December 10, 2020	Payment December 11, 2020 onwards
Members of ICSI/ICAI/ICAI-Cost	INR 1250	INR 1750	INR 2000
Students of ICSI	INR 1000	INR 1500	INR 1750
Non-Members	INR 1500	INR 2000	INR 2250
Foreign Delegates	USD25	USD30	USD35
Members above 70 years of age	INR 101	INR 151	INR 201

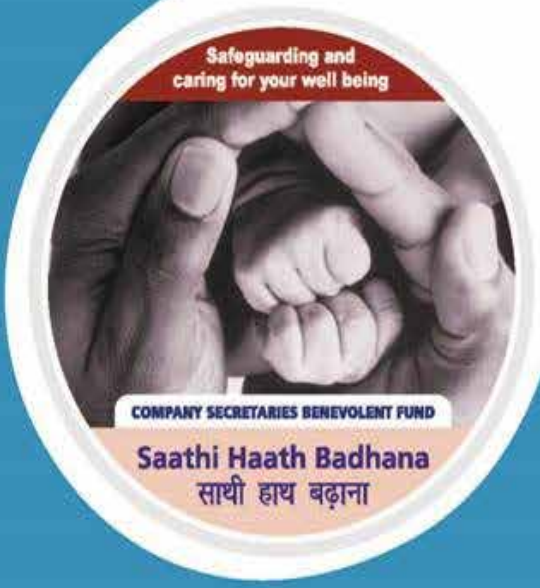
*GST @ 18% applicable on above fee
Delegates attending virtually and desirous of obtaining the delegate kit need to pay INR 500+18%GST extra for the same and INR 150 towards postage. (for Indian addressees only)
Delegate fee is payable in advance and non-refundable once received.
Delegate Registration Opening on 6th November, 2020 at 2:00 PM.
Looking forward to meet you at Indore.

Chairman, 48th National Convention Organising Committee
CS Ashish Garg, President, ICSI

Chairman, 48th National Convention Organising Sub-Committee
CS B. Narasimhan, Council Member, ICSI

THE INSTITUTE OF
Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

CSBF
COMPANY SECRETARIES BENEVOLENT FUND



What exactly is CSBF?

The Company Secretaries Benevolent Fund (CSBF) is a Society registered under the Societies Registration Act, 1860 and is recognized under Section 12A of the Income Tax Act, 1961.

The CSBF was established in the year 1976 by the ICSI, for creating a security umbrella for the Company Secretaries and/or their dependent family members in distress.

The amount of ₹ 7,50,000 (in the case of death of a member under the age of 60 years) has been increased to ₹ 10,00,000

The subscription amount is being increased from ₹ 10,000 to ₹ 12,500 soon

Is it the right time to enrol in CSBF?

CSBF is the protection you and your family need to survive the many ups and downs in life, be it a serious illness or a road accident which derails your plans for the future.

Is it a requirement?

Yes, as your dependents need the protection. Your dependents be it your parents, your spouse, or your children will have to bear the brunt of paying off your home/education personal loans and even for managing day-to-day expenses without your contribution.

If you do not want to leave behind such a situation in your absence, enrol in CSBF today.

Advantages of enrolling into CSBF

1. To ensure that your immediate family has some financial support in the event of your unfortunate demise
2. To finance your children's education and other needs
3. To ensure that you have extra resource during serious illness or accident
4. Subscription/Contribution to CSBF qualifies for deduction under Section 80G of the Income Tax Act, 1961

Become a proud Member of CSBF by making a one-time online subscription of ₹ 10,000/- (to be changed soon) through Institute's web portal (**www.icsi.edu**) along with Form 'A' available at link **https://www.icsi.edu/csbf/home** duly filled and signed.

Decide Now! Decide Wise!