Dear Members,

With great pride, we bring to you the November edition of the “IIA India Quarterly”. The IIA India Quarterly is the essential resource that all members eagerly look forward to. The Quarterly contains a mix of topics including thought provoking articles from the President and CEO of IIA India, note from the Chair of the publications committee, peer-to-peer knowledge sharing, news and updates from the Institute and its Chapters along with access to important resources.

We look forward to your letters and comments regarding our Quarterly. If you would like to contribute to this publication, kindly reach out to your respective chapter or me.

With Best Regards
Joly Joseph CA, CIA, CISA
Editor - IIA India Quarterly
Contact@iiaindia.org
Dear members and Internal Audit professionals,

Wishing all a very Happy Diwali! Diwali is the occasion to celebrate victory over defeat. It is the festival to celebrate light over darkness and awareness over ignorance! Simply put, Diwali signifies the very essence of the triumph of good over evil.

Internal Audit plays a pivotal role in ensuring the triumph of good Governance and for ensuring this, the Internal audit profession must always uphold the Code of Ethics comprising of Principles and the Rules of Conduct to demonstrate Integrity, Objectivity, Confidentiality & Competency.

As Richard Chambers shares in his blog, the Internal auditor must demonstrate strong ethical resilience and the internal audit reviews must focus on the roots, not just the trees. It is important for the internal audit professionals to be constantly aware & advocate the International Professional Practices Framework (IPPF) to provide assurance and insights with objectivity to the stakeholders.

UPDATE ON IIA INDIA GOALS

Team IIA India is driving four goals through the National Committees of the Council, through the respective Chapters and guided by the Executive Committee of the National Council, the CEO and the support Team.

LAST QUARTER UPDATE

During the last quarter, IIA India provided in-house training on Internal Auditing to the office of the NIRD and to M/S Druk Holding and Investments (DHI) Bhutan. IIA India also conducted GTM training programs in association with our training partner Achromic Point at Mumbai, Chennai, Bengaluru & Delhi. There were also Regional Conferences, Seminars, Workshops & Roundtables organized by the respective Chapters at Delhi, Hyderabad, Bengaluru, Kolkatta, Mumbai and Chennai.

Membership services are brought under the CEO’s office for better engagement with members. The QA Committee is evaluating requests for QA from members. Social media committee is disseminating knowledge bytes to the members. Advocacy Committee is working on forging relationship with other professional institutes & the Audit, Legal, Compliance Committee is focused on making your Institute a sustainable organization. As the President, I had the opportunity to deliver a session on Internal Audit at the Master Class for Directors hosted by IOD & also at the training event of GRMI (an MOU partner of IIA India).

NATIONAL CONFERENCE

IIA India - Bombay Chapter would be hosting the IIA India National Conference 2019 on January 21 & 22 at Hotel Sahara Star Mumbai. Global Chairman Mouri san and the Global president and CEO Richard Chambers along with a galaxy of international and national speakers would be addressing the delegates and participating in the Conference. This would be great opportunity for members and the internal audit community to learn and network. For registrations, please reach out to president@iiaindia.org.

I look forward to meeting you at the National Conference on 21st & 22nd January, 2019.
We have exciting times ahead for The IIA India; as well as for the internal audit profession in our country. Changes in regulatory compliances, technology disruptions, increased focus on governance & the Indian economy becoming one of the fastest growing economies globally provide all of us many more opportunities in the area of governance, risk and controls. To cater to these multiple changes, our dynamic President, Mr. S. Bhaskar has gotten off to a flying start by organizing over 10 Committees at the National Level to look after several areas including Membership Services, Training, Conferences & Events, Webinars, Publications etc., which we hope will enable us to serve our members better. A Strategic Plan for the next 3 years has also been prepared to improve our planning processes.

The IIA Global motto of “Progress through Sharing” also emphasizes the importance of TEAM work. Mr. K. Vidyadharan, a past President of IIA India, had very nicely articulated that the word TEAM also stands for “Together Everyone Achieves More”. When I was the President of the Delhi Chapter I had added that the individual letters in the word TEAM stand for “Training-Events-Advocacy-Membership”. I believe that these still remain relevant and will expound on each of these areas, briefly.

- Training: We have already initiated regular trainings with the use of Global Training Material, through The IIA Inc. Please do refer to iiaindia.org for our detailed Training Calendar. This is in addition to the events and professional development meetings taking place at Chapters. I welcome all Members to support trainings; especially if they have the experience of conducting a training programme on any particular subject or are in a position to offer their office space for small gatherings of ten to twenty-five people. The interest shown by the CGA and the Ministry of Rural Development in organizing a Certificate Course on Internal Audit with inputs from The IIA is likely to create an ongoing need for a pool of trainers across the country. A Training Policy is also on the cards.

- Events: The Mumbai, Chennai, Calcutta & Bangalore Chapters have taken a lead in organizing 1 day events, in addition to the trainings referred to above. Members are requested to block 21/22nd January, 2019 on their Calendars with the IIA Chairman of the Board, Mr. Naohiro Mouri and the President & CEO, Mr. Richard Chambers who will address the delegates. This promises to be a mega event.

- Advocacy: Our initiatives and MoUs with the CGA and the NIRD are already bearing fruit. We welcome any inputs which allow us to initiate relationships with other bodies like CII, AIMA, DMA, FICCI, ASSOCHAM etc.; these can enable us to forge new relationships, host joint events and enhance advocacy efforts.

- Membership: I earnestly urge all members to make an effort to add our numbers by referring and helping induct at least two members each before the end of this calendar year. I have no doubt that with your individual professional networking would help add momentum to our expanding activities.

- Volunteering: All of us have benefited from the profession of internal auditing over the course of our professional career. IIA welcomes those of you who can spare some of your time, resources & networking capabilities to contribute back to our profession.

- Obtaining sponsorships for IIA events from companies which are supporting or targeting our professional membership base

Rest assured that your volunteering will help your growth as a professional as well as your personal development. Interested CIAs, members & CIA students may please write in to the email id below.

We welcome your comments, feedback and support on our email id memberservices@iiaindia.org. I look forward to hearing from you and being in touch with you during 2018 - 19.
Dear IIA Members and Professional friends,

Greetings of the festive season from IIA India.

I am delighted to take up the role and responsibilities of the Chairman of the Publications Committee of IIA India for the year 2018-19. The others who are serving in this Committee are Mr. Deepak Wadhawan, former CEO of IIA India and the Chief Editor of the Newsletter from New Delhi, Mr. AR Parthasarathy, Joint Secretary of IIA India from Chennai, Mr. Chandi Bakshi, Treasurer of IIA India from Kolkata and Mr. Joly Joseph, Vice President of Bangalore Chapter of IIA India from Bengaluru.

We continue to publish the IIA India’s Newsletter every quarter. Mr. Joly Joseph will be the Editor under the overall control of the Chief Editor Mr. Deepak Wadhawan. The next edition of the Newsletter is being published in November 2018.

Our Committee has also taken up the task of publishing a Guidance Book on “Fraud Risk Management – Role of Internal Audit”. The work has just begun. The Authors will be Mr. NG Shankar, Consultant in Delhi who is former CAE of Aditya Birla Group, Mrs. Vidya Rajarao, partner of Grant Thornton from Bengaluru, Mr. KBS Manian, Chief Risk Officer of Apollo Hospitals Enterprises, Chennai and the Lead Author will be Mr. Viswanadh Kuchi, President of the Bangalore Chapter and Partner of Sudit K Parekh & Co, Bengaluru. We are planning to release the publication in the national Conference of IIA India to be held on 21st & 22nd January 2019 at Mumbai.

It would be pertinent to mention that the previous publication of IIA India on “Internal Financial Controls – Role of Internal Audit” was very well received by the IA community at large in India. I request our Members and IA Professional friends to suggest topics which will be very useful for Internal Auditors in India so that our Committee will consider your suggestions for bringing out similar publications in future.

Wishing you happy reading and best regards.

NEW RELEASES FROM THE IIA

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This publication relates the COSO Internal Control — Integrated Framework to the Three Lines of Defense Model and helps organizations enhance their overall governance structures by providing guidance on how to articulate and assign specific roles and responsibilities.</td>
<td>Who is responsible for communicating opportunities to enhance internal audit performance? When it comes to improving internal audit performance, the things that audit committee chairs hesitate to say are often the things that audit executives most need to hear.</td>
<td>Bill Shireman, President and CEO of Future 500, discusses how to find common ground between uncommon allies. Read four ways corporate Environmental, Health &amp; Safety can reduce enterprise risk, protect the brand, and earn stakeholder support in polarized times.</td>
</tr>
<tr>
<td>White Paper Supports Advocacy Efforts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New thought leadership from The IIA and IFAC examines the separate and distinct roles internal audit and the finance function play in good governance. Share United, Connected and Aligned with key stakeholders.</td>
<td>Download your complimentary copy today.</td>
<td>Download your complimentary copy today.</td>
</tr>
</tbody>
</table>
Every organization must recognize the risk of ransomware, and the Internal Auditor should be armed with the essentials of remediation and mitigation controls to address this threat and must include this guidance to clients. This article is not technical but seeks to highlight the business risk and focus on practical controls.

INTRODUCTION

Ransom or firoti, is a crime that existed in the real-life where someone is kidnapped, or taken hostage, for ransom. The criminal is usually caught when accepting the ransom, or later while spending the ill-gotten gains, or through the police network of ‘khabris’ as the crime is may have been committed by a gang or a person who knows the victim. However, real life has been overtaken by virtual life where data is key to our survival and well-being, on our computers, networks, and phones. Imagine the scenario where the organization loses all data and software and cannot access their computers – this is a threat to the very existence of the organization. (See Case Study on Maersk Lines)

Ransomware is the new age format of kidnapping, except that the target is not a high-value person but our DATA. Imagine a scenario where the hard disk in your computer (or mobile phone) has been encrypted by some unknown person and you are unable to access anything – the device or the data in it, your email, bank, internet etc. in such a situation, life and business will come to a halt. Today, ransomware is the biggest threat to any computer system, whether owned by an individual, a government, or a local or global corporation. The attack, launched by infecting the computer with a malicious software (malware), encrypts the hard disk, effectively shutting you out of the system making it un-usable, asking you to pay the ransom amount to be able to get access back. The payment is usually demanded in Bitcoins which makes the transaction practically untraceable.

So here we have a criminal, identified by an email address and a Bitcoin account number, who has just taken over your data, is unidentifiable and untraceable who may be operating from anywhere in the world, possibly be next door too. No khabi network to identify or nab the criminal and your data is as good as gone… or is it!

Ransomware is a malicious program that infects your computer, encrypts all the data on the hard disk, locks you out of your computer, then asks you to pay a “ransom” to get the decryption key. If you are on a network, it will travel quickly to infect other machines. Over the years some well-known ransomware malware are CryptoLocker, CryptoLocker.F and TorrentLocker, CryptoWall, Fusob, WannaCry, Petya, etc. The malware is usually transmitted through an infected file attachment arriving with an email, infected USB or it can spread across the network from a compromised machine. With mobile phone becoming a large part of our computing activity, malicious apps and computer programs are suspect infection points.

The May 2017 global infection by WannaCry (followed by Petya/NotPetya) brought the scepter of ransomware onto mainstream discussions when organizations realized that this threat is real, very dangerous, and can hit anyone an individual, a government, a local or global corporation. Why would you or your organization land up in such an extremely hot soup? And the reasons are not many!

An infected document (DOC, PDF, XLS, PPT, EXE, ZIP etc.) comes into your IT environment, is opened by someone and the attack is unleashed. Infected documents can travel into your environment as attachments with spam mails or may be brought...
on USB by any employee. Someone opened a spam mail and then clicked the malicious URL or opened an infected attachment. You may be infected with the malware when visiting a compromised website (this attack is also known as a “drive by download” attack; or if it is a site commonly visited then it can also be termed as a “watering hole attack”). Shadow IT risk visited your network through a user who downloads and installs unauthorized software (on the desktop or on mobile) which was actually malicious.

Unpatched system or software in the network is compromised by the criminal taking advantage of the known vulnerability. While starting mitigation, in the event of an attack, it is necessary to file a report with the nearest Cyber Police Station, and report to the regulators.

Ransomware infection moves fast across the network so the moment you know, the first act should be to take the machine, and any other infected ones, off the network. Carry out an analysis to identify the ransomware type so as to be able to plan the remediation steps. Identify the source of the infection if possible (email / USB / App etc) and isolate the same. Carry out search across the network to identify any other machines which are seemingly not attacked, to ensure they are clean and do not have a copy of the malware.

Response has to be quick and follow a planned mitigation / remediation plan. It does not matter whether you are hit through a document or website any other infection method – the first advice is “don’t pay” take a bitter pill and rebuild your system and data. The rationale for this advice is that you cannot be sure that you will get the decryption keys or retrieval instructions from this unknown, unidentifiable criminal. Remember there is no honor or ethics among thieves, especially totally anonymous ones.

Even if the criminal sends the keys, this is a risk you will be just lucky to be able to retrieve the data in good, usable (pre-ransomware) format. As such, this is a chance you are going to take which may cost you as much in cash and retrieval effort. Might as well rebuild, however, let us consider the risk scenarios and decide:

**OPTION # 1 ‘TO PAY’**

Your money is in their kitty and now these guys don’t respond. Remember you only have an email address which would have been set up only for this transaction. The criminals sent you the decryption key and instructions but it doesn’t work or gives you gobbledygook output. You cannot sue them for breach of contract!

The decryption keys and instructions worked and you got your system back. However, now your file system is (possibly) all messed up which usually happens when you are retrieving data, plus, your applications (software) doesn’t work and you have to do a fresh installation and configuration. This is still a lot of effort and time to actually get back your data and come back to normal. Remember that decryption is time consuming. So, if you pay, it is no guarantee that you will come out of the black hole or would save in costs.

**OPTION # 2 ‘DON’T PAY’**

Good! You have not paid and contributed to the well-being of a criminal. This will seem to be a tough decision to make but it is the best decision under the circumstances. Now let’s get to work. First, we identify the ransomware strain and attempt to recover our files, using commercial or open source tools and guidance (https://www.nomoreransom.org/en/index.html). Remember you may need professional help of forensic and incident response professionals. If this fails, you have to rebuild your system. Replace the hard drive and reinstall software programs.

Restore data from the backup files (I hope you have a good backup). If you do not have any backup, then life is going to be tougher as you will have to collect payment and contract information from your business associates and will have to build the business ecosystem from scratch. Whether or not you have a backup, remember take this as a fresh start in ‘life’ and take advantage of the situation and plan the storage appropriately, depending on the classification of the data (critical / non-critical / public). As risk professionals, we all know that there is opportunity in every risk!

As an auditor, it is necessary for you to flag this risk to your clients and advise them to ensure mitigating controls are enabled. Relevant and necessary policies and procedures must be developed and maintained for Risk Management, Backup & Testing, Patch Management, Security Architecture review, Security Awareness, BCP/DR, Crisis Communication, and Incident Response. Auditors must ensure that these policies address the operational requirements for ransomware mitigation. (For example, the Backup Policy should include well-defined controls and processes for each type of backup (critical, non-critical etc.), the periodicity of backup and testing, comprehensive test plans, storage location(s), access rights).

1. Backup, backup and backup - This is the primary mantra for ransomware mitigation. At the very least, sensitive or critical data should be backed up. It is industry fact that backups are successful in no more than 42% instances (Spiceworks report) so it is essential that backups are periodically tested and that tests should include restoration, data integrity check, and access rights and security of the storage location. Good guidance is available for backup from
US CERT in the form of a 3-2-1 backup strategy (download link provided in the resource list).

2. Critical machines should always be isolated from the network. This will help avoid infection spreading to these machines, as the malware travels laterally across the network.

3. System patching and updation - Software including anti-virus, anti-malware installations and spam filters must regularly updated. Anti-ransomware solutions can be considered for inclusion in the security architecture, based on a risk assessment.

4. Awareness and training - It is of utmost importance that users across the organization are sensitized to the risk of ransomware attacks and the threat to the organization. The awareness sessions must be designed to impart learning on how to identify and avoid spam emails, malicious documents / links and how to react in the unfortunate event of having clicked one. Most importantly – NEVER to open any spam!

5. Reporting and Response - This must be swift to limit damage. It means priority is given to containment and response and that the blame game or finger pointing be kept for later.

6. Management posture - Must be sensitized to the reality of ransomware and to support anti-ransomware activities. Attack services are easily available and anyone with animosity towards the organization can buy Ransomware-as-a-Service or put a “supari” on the company.

7. Email security through a Sender Policy Framework (SPF) for your domain – This is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes (was included in the previous month article on Business Email Compromise).

**DID YOU KNOW**

The WannaCry attack “nearly” killed the $37 bn Maersk Lines (2017), infecting their computers across the world, rendering them useless. So bad was the infection that, after a global search, they could find only one healthy system in Ghana out of the 130 countries where they had operations. This system was not infected because it was not online due to a power cut. The machine was carried to UK via Nigeria because no Maersk employee in Ghana had a UK visa. Maersk lost about $ 300 million in costs over a 15 day recovery period – they had to re-install 4,500 servers and 40,000 PCs.

The ripple of this attack hit Jawaharlal Nehru Port (JNPT) and practically shut down their operations as (apparently) Maersk port management system is used at JNPT.

**REFERENCES**

i. Ransomware information: https://en.wikipedia.org/wiki/Ransomware

ii. Ransomware chart 2005/16: https://blog.barkly.com/hubfs/Ransomware_discoveries_chart.png?t=1539370135449


viii. header image sourced and re-purposed from https://www.fingent.com/blog/making-sense-recent-ransomware-attacks-wannacry-malware
CLOUD COMPUTING AND RISK BASED INTERNAL AUDIT

The average cloud user connects to the cloud using the internet and does computing tasks, or runs applications, or stores data, many a time not realizing that he or she is actually using resources not available on the local host. Common cloud services available to users are Dropbox, kindle, Facebook, Twitter, Pinterest, Google etc. The most popular type of cloud service called software as a service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the internet. The cloud requires an internet connection, an account (created with a user name and a password) and an agreement to the terms and conditions of the service. So in short cloud computing is computing and software resources that are delivered on demand, as services which have evolved from on-premises computing to cloud computing (somewhere on the internet and the location is not known to the user). Traditionally computer storage was the internal or hard drive storage (c: drive) on a computer which was used for storing programs, documents, pictures, videos, presentations, etc. All content was stored on that specific computer and the content could not be accessed from another device or computer.

Traditionally programs were purchased and loaded into each computer which needed to run the program. This was followed by external storage which allowed the content to become mobile by being saved to the external storage device which could be used on any compatible computer (like cd or pen drives). The next development was the networked storage where multiple workstations could talk to a single unit that stored information and data called the network drive. Content could be stored or retrieved from the network storage by any of the connected workstations. Like a network file server.

Now we have the cloud storage facility where the user creates an account (with a user name and password) and the content lives with the account in the cloud where any computer connected to the internet can access the content if the credentials are given. Further documents can be synchronized between the device and the cloud storage to ensure that the changes made to the content using one device will be visible when the content is accessed by a different device with the same account credentials. Documents can be created using accounts provided by service providers such as google docs, skydrive etc.

Benefits of cloud storage:
- Saving Large Files
- Multiple file types – Photos, videos, presentations, docs
- Back-up of stored files
- Nothing to forget (thumb drive, cd)
- File Sharing
- Access from devices
- Project collaboration

CLOUD COMPUTING

Cloud storage (where it was a repository for data) evolved into Cloud Computing (where software could be executed from a cloud storage server) which is a general term used to describe a new class of network based computing that takes place over the Internet, which is basically a step from Utility Computing. It can be described as a collection / group of integrated and networked hardware, software and Internet infrastructure (called a platform) using the Internet for communication and provides hardware, software and networking services to clients.

These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Application Programming Interface). In addition, these platforms provide on demand services that are always on, anywhere, anytime and anyplace. The users (general public, enterprises, corporations and businesses markets) pay for use and as needed, and the services and storage can be scaled up and down both in terms of capacity and functionalities.

CLOUD SUMMARY

Cloud computing is an umbrella term used to refer to Internet based development and services and a number of characteristics define cloud data, application services and infrastructure:
- Remotely hosted: Services or data are hosted on remote infrastructure.
- Ubiquitous: Services or data are available from anywhere.
- Commodified: The result is a utility computing model similar to that of traditional utilities, like water and electricity - you pay for what you would want!
So we can now define Cloud Computing as:

- Shared pool of configurable computing resources
- On-demand network access
- Provisioned by the Service Provider

The common characteristics can be summarized as massive scale of operations; homogeneity; virtualization; low cost software; resilient computing; large geographic distribution; service orientation; advanced security; on demand self-service; broad network access; resource pooling; rapid elasticity and measured service.

CLOUD SERVICE MODELS

SAAS MATURITY MODEL

Software as a Service (SaaS)

SaaS is a model of software deployment where an application is hosted as a service provided to customers across the Internet. SaaS eliminates the burden of software maintenance/support but users relinquish control over software versions and requirements.

Virtualization

Virtual workspaces are an abstraction of an execution environment that can be made dynamically available to authorized clients by using well-defined protocols, provide resource quota (e.g., CPU, memory share) and manage software configuration (e.g., O/S, provided services). Virtualization is implemented on Virtual Machines (VMs) which are an abstraction of a physical host machine. The Hypervisor intercepts and emulates instructions from VMs, and allows management of VMs (like VMWare, Xen, etc.) and provide infrastructure APIs / plug-ins to hardware/support structures. VM technology allows multiple virtual machines to run on a single physical machine.
ADVANTAGES OF CLOUD COMPUTING

- Lower computer costs
- Instant software updates
- Improved document format compatibility
- Unlimited storage capacity
- Increased data reliability
- Universal document access
- Latest version availability
- Easier group collaboration
- Device independence
- Applications and documents are available on portable device

DISADVANTAGES OF CLOUD COMPUTING

- Requires a constant Internet connection
- Features might be limited
- Stored data might not be secure
- Stored data can be lost (there is no local backup).
- HPC (High Performance Computing) Systems may not be available from cloud service providers
- Each cloud system uses different protocols and different APIs and it may not be possible to run applications between cloud based systems (For eg. Amazon has created its own DB system (not SQL 92), and workflow system

RISKS IN CLOUD BASED COMPUTING

1. POLICY AND ORGANIZATIONAL RISKS
   R.1 Lock-in
   R.2 Loss of governance
   R.3 Compliance challenges
   R.4 Loss of business reputation due to co-tenant activities
   R.5 Cloud service termination or failure
   R.6 Cloud provider acquisition
   R.7 Supply chain failure

2. TECHNICAL RISKS
   R.8 Resource exhaustion (under or over provisioning)
   R.9 Isolation failure
   R.10 Cloud provider malicious insider - abuse of high privilege roles
   R.11 Management interface compromise (manipulation, availability of infrastructure)
   R.12 Intercepting data in transit
   R.13 Data leakage on up/download, intra-cloud
   R.14 Insecure or ineffective deletion of data
   R.15 Distributed denial of service (DDoS)
   R.16 Economic denial of service (EDOS)
   R.17 Loss of encryption keys
   R.18 Undertaking malicious probes or scans
   R.19 Compromise service engine
   R.20 Conflicts between customer hardening procedures and cloud environment

3. LEGAL RISKS
   R.21 Subpoena and e-discovery
   R.22 Risk from changes of jurisdiction
   R.23 Data protection risks
   R.24 Licensing risks

4. RISKS NOT SPECIFIC TO THE CLOUD
   R.25 Network breaks
   R.26 Network management (ie, network congestion / mis-connection / non-optimal use)
   R.27 Modifying network traffic
   R.28 Privilege escalation
   R.29 Social engineering attacks (i.e, impersonation)
   R.30 Loss or compromise of operational logs
   R.31 Loss or compromise of security logs (manipulation of forensic investigation)
   R.32 Backups lost, stolen
   R.33 Unauthorized access to premises (including physical access to machines and other facilities)
   R.34 Theft of computer equipment
   R.35 Natural disasters

RISK MATRIX:

The readers may also refer to:
https://cloudsecurityalliance.org/
Spreading wings to Bhutan

In a path breaking initiative, The IIA India, conducted a five-day certificate program on Internal Audit for Druk Holding Investments Limited (DHIL) at Phuentsholing, Bhutan.

The course was attended by 24 Internal Auditors/Finance executives from the 19 group companies of DHIL with experience levels ranging 1 year to 20+ years. Trainers from IIA India included Mr. Vishwanadh Kuchi, Chair, Training Committee, IIA India, Mr. N.G. Shankar, Ex-President-Internal Audit, Aditya Birla Group and Mr. Nikhel Kochhar, CEO, IIA India.

The trainings were highly appreciated by the participants.

Fraud Risk Seminar by Chennai Chapter

The One-day seminar on “Fraud Risk Management – Role of Internal Audit” was organised by IIA Madras Chapter on 4th October 2018 at Hotel Rain Tree, Anna Salai, Chennai.

It was well attended by 77 delegates drawn from a cross section of industries and practicing IAs.

There were two technical sessions and one panel discussion. The faculties were Mr. NG Shankar, Consultant at Delhi, former CAE of Aditya Birla Group, Ms. Vidya Rajarao, partner of Grant Thornton, Bengaluru, Mr. KBS Manian, Chief Risk Officer of Apollo Hospitals, Chennai and Mr. AR Parthasarathy, partner of RGN Price & Co, Chennai.

Annual Conference by Delhi Chapter

“Staying Relevant in the Automation, Compliance and Technology Landscape - The Time to ACT is Now”.

The Delhi Chapter also organized an Annual Conference on 24th August on the topic “Staying Relevant in the Automation, Compliance and Technology Landscape- The Time to ACT is Now”. The Conference aimed at familiarizing the participants with the technology led changes that are happening and to equip themselves with the changes to stay ahead of the curve. The Conference witnessed more than 180 delegates attending and more than 30 speakers conversing on a range of topics. The discussions at the Conference were thought provoking and interesting.
Digital Auditor by Kolkata Chapter

The Institute of Internal Auditors India, Calcutta Chapter organized an one day seminar with the theme “The Digital Auditor “on 5th October 2018 in Kolkata. The seminar was divided into 3 sections, 2 technical sessions and one panel discussion. The seminar keynote address was given by Mr. Sanjay Kr Das, Dy Secretary Information Technology, Govt. of West Bengal. The president of Calcutta chapter Mr. Debshis Ghosh gave the inaugural speech introducing audience to the theme of the seminar and outlining the transformation from traditional to digital auditing.

Two eminent speakers deliberated on Evolution of Audit which was moderated by Jt secretary of IIA Calcutta Chapter. Next was the Panel discussion on “Cyber Security & Role of Auditors” followed by the final session on “Impact of Digitization on Internal Audit”. The session was moderated by Treasurer IIA India. The seminar ended with a vote of thanks from Secretary of IIA Calcutta Chapter to all the speakers who shared their precious knowledge with all of us. Also all attendees who contributed and participated to the success of the event. The seminar was attended by 60 participants from various companies like CESC, Berger Paints, Emami, Mjunction, DVC, Tata Metaliks etc.

CAE roundtable by Bangalore Chapter

The Institute of Internal Auditors India, Bangalore Chapter along with SAP organized an evening with CAE and other senior leadership around the theme “Digital Audit Transformation Day” on 5th October 2018 at the Ritz Carlton in Bangalore.

The evening started with an interesting talk by Kevin McCollom and Murali N from SAP on the topic - Impact of the Digital Economy on risk and compliance. This was followed by a panel discussion and the topic was “Embracing Digital: Auditing digital transformations and using digital to transform auditing” moderated by Joly Joseph, VP of IIA Bangalore Chapter. The panel comprised of Balaji Ranganathan, VP Internal Audit from Fidelity, Amit Bajoria, VP Internal Audit from Wipro and Prem Kumar, Associate Director om PWC. The discussion was around the differences internal audit teams must embrace in this new journey, new skillsets needed, acceptance and responses from Management and Audit Committees and the challenges for CAE in the future.

Seminars by Mumbai chapter

IIA Bombay Chapter along with Riskpro has organized a one-day seminar on 7-Sep-18 titled “Auditing Emerging Trends”. Emerging topics such as General Data Protection Rules, India Data Protection Bill, Implementing GDPR in Indian companies, Vendor Risk Management and blockchain were discussed. A captivating panel discussion on “Will blockchain will change the way we do internal audit” has elicited mixed responses from attendees. This event was attended by more than 40 delegates.

Another interesting event on Cyber Security and Role of Internal Audit is organized on 27-Oct-2018. A number of pressing topics such as Cyber Security framework and governance, Threat and Identification of threats, responding to cyber security threats, Auditing Cyber Security and Regulatory aspects of Cyber Security were discussed. This event was attended by more than 40 delegates. Two webinars organized on “Million wings of Internal audit” and “SAP Security control” has received overwhelming response from India as well as abroad.
Mark your Calendar

Mon Jan 21 @ 8:00AM - 05:00PM
IIA India and Bombay Chapter Annual Conference, 2019 - Emphasize the Basics; Elevate the Standards

Video Watch

2018 IIA Chairman’s Message
Click Here

Corporate Governance – Role of Internal Auditors organized by IIA Bombay & BCAS by Nawshir Mirza
Click Here

Internal Audit Jobs

Check out the latest internal audit jobs.
Click Here

Reach out to us for Volunteering

Please volunteer at your local chapter. For your Chapter information
Click Here

Training Programmes

Check out the latest IIA held training programmes.
Click Here

Letter to the Editor

We look forward to your emails. Reach out to us at contact@iiaindia.org

Disclaimer:

The IIA India quarterly is a digital newsletter for the general knowledge on internal audit, circulated primarily to its members. The articles are the personal views of the authors. IIA India and its officers neither endorse nor are liable for any views or actions taken based on this newsletter. Before proceeding further do take professional advice. No part or extract of this issue may be reproduced without the permission of the author and IIA India in writing.