In Search of Excellence
A Newsletter of RTI, Chennai
April 2020 –March 2021

April 2021

लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

From Director General's Desk

In G.K. Chesterton's short story titled "Angry Street a bad dream", the protagonist walks down a street every evening from his workplace for a little over forty years. One evening, he starts panting while walking on the same street and realises that the street has developed a steep incline and he is actually climbing up. The street is suddenly imbuing with familiar and unfamiliar points. He is thoroughly shaken as the street appears to be hanging up in an empty space! He sees a man standing in the balcony of a house that wasn't there all these years and asks him for the name of the street and if it leads to the place that it has led to all these years. The man confirms the name of the street. Strangely, he says that the street leads to the place that it has led to all these years sometimes but that day, it was leading to the heaven! He says in an apocalyptic tone, "Remember always that there is one thing that cannot be endured by anybody or anything. That one unendurable thing is to be overworked and also neglected. The street has gone tired of your tireless insolence and it is bucking and rearing its head to heaven."

The world turned out to be like the angry street in March-April of 2020 in the wake of the Covid-19 pandemic when all of us were turned away lock, stock and barrel. What was taken for granted as normal and beyond change turned topsy-turvy.

With the implementation of lockdown, this small microcosm called the RTI also had to suspend classroom training. As we all know, the pandemic year also brought the world together like never before albeit through online medium. Here at RTI, we harnessed the immense possibilities of the online mode of training from May 2020. The trainers and the trainees adapted to the online training method quite well. One of our faculty members has written a piece in this newsletter about this whole new way of training with undertones of humour.

We were able to complete all the planned courses in the online mode. We imparted training to 1355 officials on various topics and skills during the year through 63 courses.

We also conducted 3 Pan-India courses during the year on the three Knowledge Centre (KC) topics assigned to this RTI. Sixteen IA&AS officers attended 4 courses including the three Pan-India courses on KC Topics.

We conducted a new course on 'Data Analytics using R' during the year to enhance the skill set of our trainees.

We have also prepared a STM on 'Data Analytics using R' and sent to headquarters.

Besides, the infrastructure facility of the Institute was shared with other offices in the station for conducting workshops/ conferences /in-house training programmes. One of the IS labs was used for conducting online GST Audit by the Office of the Principal Director of Audit (Central) Chennai since October 2020.

The details of training courses conducted during the year are as under:

Type of course	No. of courses	No. of trainees	No. of training days
General	36	913	190
IS	24	442	110
Total	**63**	**1355**	**300**

Online training also opened up the opportunity of roping in expert faculty across the country like -
➢ Sri. Amitabh Datta, Adjunct Professor, National Institute of Financial Management, Faridabad
➢ Smt. Jayashree Venkatesh, Ecologist, Care Earth Trust, Chennai
➢ Sri. Devkumar Rajwani, Dy.Commissioner, GST Dept.,(Anti-profittering), New Delhi.
➢ Sri. V Thirunavukarasu, Chief Conservator of Forests, Tamil Nadu
➢ Sri. S. Murali, GM(Finance), Chennai Metro Rail Limited
➢ Sri. P K Acharya, GM(Finance), Neyveli Lignite Corporation
➢ Sri. Raghunath, Vice Principal, RBI Staff College, Chennai
➢ Sri. M. Sathyakumar, CEO & Founder, Tycoon + Advisors, Chennai
➢ Smt. Karthikeyani, JT Commissioner, Commercial Taxes Dept. Govt. of Tamil Nadu, Chennai.
➢ Dr. B. Srinivasan, IRAS, FA&CAO (Retd) , Indian Railways
➢ Sri. Chidambaram, Registrar, IIITDM, Kanchipuram.

This Institute would strive to provide need-based and quality training as always. We sincerely hope that we would come out of the clutches of the covid pandemic situation and get the trainees here to the RTI.

S. Rajani
Director General

What is inside

Regional Training Institute, Chennai


Lush green environment in RTI Chennai

Big Data and Ethics

The IT Act defines "Data" as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

Previously in most cases, data stored was validated for relevance and accuracy and followed a pattern related to business needs. However, with computing power not being a limitation, the trend turned more towards capture of all types of data (including click information, browsing and viewing details) and trying to make a pattern out of it for visualization and analysis. Further with the growth of cheap storage space, data storage was not an issue. The buzzword was store the information and forget about deleting it. This lead slowly to the era of Big Data.

What is Big Data

Big data is often characterized by the 3Vs: the large *volume* of data in many environments, the wide *variety* of data types stored in big data systems and the *velocity* at which the data is generated, collected and processed. These characteristics were first identified by Doug Laney, then an analyst at Meta Group Inc., in 2001
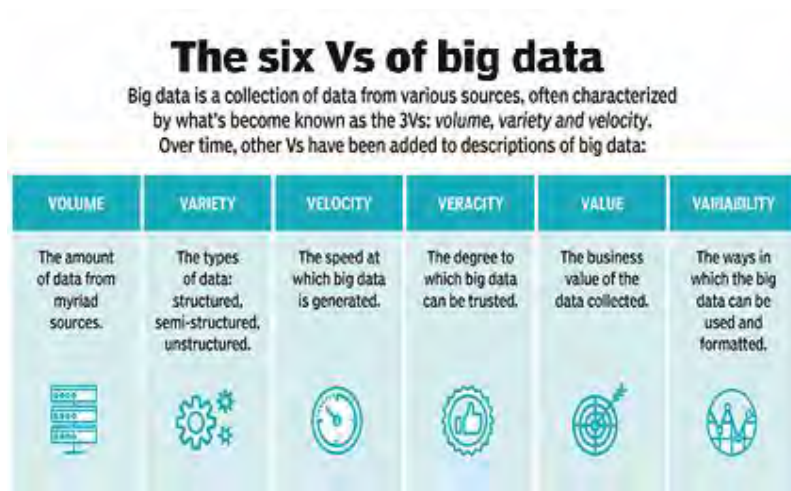
We live in an age when the amount of data we expect to be generated in the world is measured in exabytes and zettabytes. By 2025, the forecast is that the Internet will exceed the brain capacity of everyone living on the entire planet.

More recently, several other Vs have been added to different descriptions of big data, including *veracity*, *value* and *variability*.

Although big data doesn't equate to any specific volume of data, big data deployments often involve terabytes (TB), petabytes (PB) and even exabytes (EB) of data captured over time.

Big data comes from myriad different sources, such as business transaction systems, customer databases, medical records, internet clickstream logs, mobile

applications, social networks, scientific research repositories, machine-generated data and real-time data sensors used in internet of things (IoT) environments. The data may be left in its raw form in big data systems or pre-processed using data mining tools or data preparation software so that it is ready for particular analytics uses.

Using customer data as an example, the different branches of analytics that can be applied with the information found in sets of big data include the following:

- Comparative analysis: This includes the examination of user behaviour metrics and the observation of real-time customer engagement in order to compare a company's products, services and brand authority with those of its competitors.
- Social media listening: This is information about what people are saying on social media about a specific business or product that goes beyond what can be delivered in a poll or survey. This data can be used to help identify target audiences for marketing campaigns by observing the activity surrounding specific topics across various sources.
- Marketing analysis: This includes information that can be used to make the promotion of new products and services more informed and innovative.
- Customer satisfaction and sentiment analysis: Information gathered in its entirety can reveal how customers are feeling about a company or brand, if any potential issues may arise, how brand loyalty might be preserved and how customer service efforts might be improved.

The positive aspects of analysing this huge tranche of information is manifold, but what about the risks.

Big Data Ethics

Big data raises personal privacy concerns. Why? With the advent of IOT, where devices are smart and can capture information about anything, from behaviour to various activities done, it generates new questions about personal identity, notably who owns our personal data and how the increased presence and availability of more data would influence our reputations. For both individuals and organizations, four common elements define what can be considered a framework for big data ethics:

Identity	What is the relationship between our offline identity and our online identity?
Privacy	Who should control access to data?
Ownership	Who owns data, can rights to it be transferred, and what are the obligations of people who generate and use that data?
Reputation	How can we determine what data is trustworthy? Whether about ourselves, others, or anything else, big data exponentially increases the amount of information and ways we can interact with it. This phenomenon increases the complexity of managing how we are perceived and judged.

Which means this framework has the potential to inform both the benefits big data provide and the potential risks from unintended consequences for a truly staggering number of people. *As an example, New York Judge Gary Brown recently found that an IP address is not sufficient evidence to identify*

*copyright infringers (*https://www.csoonline.com/article/2226598/ip-address-does-not-identify-a-person-judge-tells-copyright-troll-in-bittorrent-ca.html*).* Although this legal finding was focused on copyright issues, it could have far-reaching implications for questions about all four elements of big-data ethics. If a person is not an IP address (and who, really, ever thought they were identical?), then can any data generated via a specific IP address be legitimately associated with a single, unique individual?

A realistic scenario illustrates some of the challenges people and organizations face. Imagine that an elderly relative's glucose and heart monitoring device shares the same IP address as the rest of your household. As a matter of course, all data from those medical devices is captured and stored by a healthcare provider. Now imagine that through an internal data leak, the hospital inadvertently mixes up their medical condition with your own. After all, you both live at the same address, could be the same gender, and might have the same last name.

Codes of ethics and conduct related to computers, analytics and big data

IEEE	Ethics and Member Conduct (www.ieee.org/about/ethics.html)
ACM	ACM Code of Ethics and Professional Conduct (www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct)
British Computer Society	Code of Conduct for BCS Members (www.bcs.org/upload/pdf/conduct.pdf)
Data Science Association	Data Science Code of Professional Conduct (www.datascienceassn.org/code-of-conduct.html)
INFORMS for the Certified Analytics Professional	Code of Ethics for Certified Analytics Professionals (www.informs.org/Sites/Certified-Analytics-Professional-Program/CAPs/CODE-OF-ETHICS)
American Statistical Association	Ethical Guidelines for Statistical Practice (http://biostat.mc.vanderbilt.edu/wiki/pub/Main/HeitmanSeminarMay08/ASAEthicalGuidelinesforStatisticalPractice.pdf)

Big data can reconstruct your entire travel history anywhere on the planet. It supplies the information necessary to tie together intentionally disparate facets of your personality in ways we sometimes cannot fully control. Pictures of you on spring break are presumably not intended to be considered as relevant material when applying for a job, and big data has significantly changed how reputation is managed in such situations. This data trail is just one example of how big-data technologies allow broader and deeper insight into human behaviour and activity than ever before.

Because the data is frequently data about people and their characteristics and behaviour, the potential use and abuse of this acquired data extends in a great many directions. Direct benefits are now being realized, but concerns about the consequences of having personal data captured, aggregated, sold, mined, re-sold, and linked to other data (correlated) are only now beginning to be felt and expressed. And these risks are not just limited to individual people. They apply equally, if not more, to organizations. Corporations are not in the business of harming their customers. Hospitals are not in the business of violating their patients' confidentiality. Non-profit research facilities are not in the business of sharing their test subjects' personally identifiable information. Yet, through the normal course of everyday business operations, which increasingly utilize big-data technologies, the risk of various harms increases. And the type, size, and impact of those risks are difficult to determine in advance. We have, as a society, only just begun to understand the implications of the age of big data.

To believe that a computer program is information neutral is a fallacy and myth given the fact that they are instructed to behave in a certain way. To consider checks and balances one relevant question could be whether data audit and audit of personnel handling the data is relevant or not.

Relevance of Data Handling Audit

A key task in the evaluation of current practices is a thorough audit of data handling practices. A wide variety of organizational or business units touch many aspects of data handling. A rigorous audit will include process owners from each business group involved in any aspect of how data is handled. Considerations include:

- Who within your organization has access to customer data?
- Are they trustworthy?
- By what methods have you determined them to be trustworthy?
- What processes are in place to ensure that breaches of trust will be noticed?
- What technical security measures are taken with data?
- Are they sufficient for the purposes?
- Who outside of your organization might be interested in gaining access to the data you hold?
- How strong is their interest, and what means might be at their disposal to breach your security?

The truth is that Big-data technology has no value framework. Individuals and corporations, however, do have value systems, and it is only by asking and seeking answers to ethical questions that we can ensure big data is used in a way that aligns with those values.

Legal Position in India

The Information Technology Act (2000), amended by the Information Technology (Amendment) Act (2008) contains provisions for the protection of electronic data. The IT Act penalizes "cyber contraventions" which attract civil prosecution under section 43 (a) to (h) and "cyber offences" which attract criminal action under sections 63 to 74. The former category included gaining unauthorized access to, and downloading or extracting data from, computer systems or networks. The latter covers "serious" offences like tampering with computer source code, hacking with intent to cause damage and breach of confidentiality and privacy.

In April 2011, the Ministry of Communications and Technology published four sets of rules implementing certain provisions of the Information Technology (Amendment) Act (2008). Of relevance to the issue of data protection are the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) (SPD) Rules (2011). The SPD Rules were framed under section 43A of the IT Act, and set out procedures for corporate entities which collect, process or store personal data (including sensitive personal information). These rules also distinguish "personal information" from "sensitive personal information".

Draft legislation called the Privacy Bill was released in 2011, which recognized an individual's right to privacy. Various iterations of this bill were released over six years, the most recent of which was the Data Privacy Bill, 2017. However, this bill did not pass into a law. Subsequently, the Supreme Court recognized the right to privacy as a constitutionally guaranteed fundamental right in 2017. In August 2017, the government empanelled a ten-member committee of experts under the chairmanship of a retired Supreme Court judge to identify key data protection issues in India and recommend methods of addressing them. The committee submitted a nearly 200 page report containing a "data protection framework" along with the draft Personal Data Protection Bill, 2018. The Minister of Electronics and Information Technology tabled the Personal Data Protection Bill 2019 in the Lok Sabha on 11 December 2019 and the same is being analysed by a Joint Parliamentary Committee in consultation with various groups. The Bill covers mechanisms for protection of personal data and proposes the setting up of a Data Protection Authority of India for the same.

Data protection is also covered in the following laws

- The Copyright Act (1957) – The act protects intellectual property rights in different types of creative work including literary works, and the term "literary work" statutorily includes computer databases, copying a computer database, or copying or distributing a database.
- The Indian Penal Code (1860) – Provisions could be made applicable to prevent theft of data. The offences of theft and misappropriation technically apply only to movable property under the Indian Penal code, but the term "movable property" has been defined to include corporeal property of every description except land or property that is permanently attached to the earth.
- Article 21 of the Indian Constitution – Protects an individual's right to life and personal liberty. Article 300A of the constitution also guarantees the right not to be deprived of one's property except by authority of law, so if the data in question is regarded as property this provision is relied upon.
- Further any individual is at liberty to initiate any action in tort for breach of privacy.
- Business Process Outsourcing Units implement self-regulatory processes, such as the BS 7799 and the ISO 17799 standards, to standardize information security management and restrict the quantity of data made available to employees.
- The Reserve Bank of India periodically issues guidelines to maintain the confidentiality and privacy of client information. In 2006 the Banking Codes and Standards Board of India was established to evolve a set of voluntary norms which banks must enforce themselves through internal grievance redressal mechanisms within each bank.
- The Medical Council of India has set out the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (Code of Ethics Regulations, 2002). These rules govern various issues, including doctor-patient confidentiality, the collection of personal data from patients, issues of consent and the extent to which invasive procedures may be conducted.
- Similarly the Securities and Exchange Board of India is a securities market regulator which required securities market intermediaries to maintain confidentiality of client data, including personal data.

Conclusion

The goal for data ethics is to take a clear look at what is done with data and whether data is safe. The implications of data misuse does not stop only with organisations, but also have implications on National Security too.
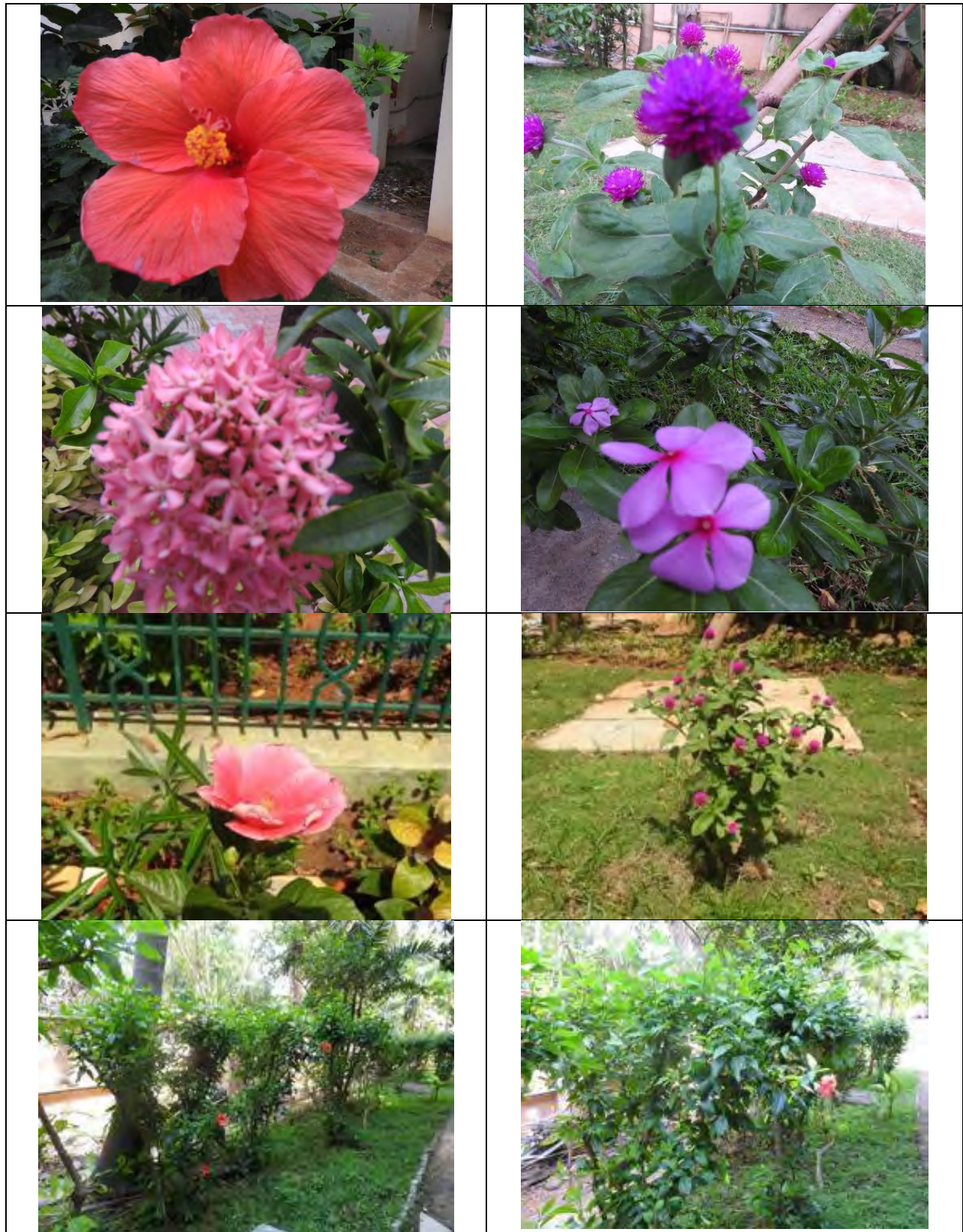
Recently, on 03 September 2020, Government of India blocked 118 mobile applications, including PUBG, in the interest of "sovereignty and integrity of India, defence of India, security of state and public order" by invoking Section 69 of Information Technology Act. The banned apps include Baidu, Baidu Express Edition, Tencent Watchlist, FaceU, WeChat Reading, Ludo All Star, Alipay and Tencent Weiyun, besides PUBG Mobile and PUBG Mobile Lite, according to an official statement. The press release stated that "The Ministry of Electronics and Information Technology, Government of India, invoking it's power under section 69A of the Information Technology Act read with the relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules 2009 and in view of the emergent nature of threats, has decided to block 118 mobile apps since in view of information available they are engaged in activities which are prejudicial to the sovereignty and integrity of India, defence of India, security of state and public order,"

The message is clear: countries, organisations and the people must decide for themselves how far they must extend cooperation to various data-handling practices in order to protect themselves. The complete data exhaust trail of big data can reach dozens, even hundreds, of other organizations. A thorough understanding of which third parties have access to data (through sales, storage, sharing, or any other means) must be developed and documented up to and including the point ethical values dictate. Till such time comprehensive legislations are not in place, which afford to be unaware what digital footprint he/she will leave, which can be analysed in a different way subject to varying interpretations.

References

https://searchbusinessanalytics.techtarget.com/definition/data-preparation
https://searchdatamanagement.techtarget.com/definition/Hadoop
https://searchdatamanagement.techtarget.com/definition/NoSQL-Not-Only-SQL
https://searchsqlserver.techtarget.com/definition/SQL
https://searchdatamanagement.techtarget.com/definition/data-warehouse
https://www.webopedia.com › TERM › data
https://en.wikipedia.org › wiki › Data
https://www.diffen.com › difference › Data_vs_Information
https://searchdatamanagement.techtarget.com/definition/big-data
https://www.commit-nl.nl/sites/default/files/Ethics%20of%20Big%20Data_0.pdf
https://iclg.com/practice-areas/data-protection-laws-and-regulations/india
https://en.wikipedia.org/wiki/Personal_Data_Protection_Bill_2019
https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
Dan – Ethics for big data Analtyics.pdf

Information security Awareness

Lately there have been many instances of people losing money on account of information technology backed social engineering scams like Phishing, Vishing and impersonation. So what are these and how to be wary of such attacks?

Phishing is the practice of sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information. Vishing is the practice of eliciting information or attempting to influence action via the telephone, which may include use of technical tools for phone spoofing. Impersonation is the practice of pretending as another person with the goal of obtaining information or access to a person, his or her bank accounts, company details or computer system.

How do they do it?

Generally, people receive a phone call from callers posing as company or bank official. They would be drawn into a conversation about revealing information. The common reasons cited for asking details – reactivation of cards/accounts for encashing of reward points, sending a new card, linking the account with Aadhaar, unblocking the card or renewal of a card. Slowly information would also be sought on one time password for renewal, credit/debit card number, CVV number, expiry date, Internet banking login id, password, etc. in short all the details that are generally used to conduct online transactions.

In most cases unsuspecting people believing that their card is being renewed or their discount voucher is being generated reveal the OTP received to the caller, without realising that the caller has already his/her bank details and password and the OTP is used for transferring money from their accounts.

So how to stay safe.

The thumb rule is never divulge your card number, CVV or OTP to anyone claiming to be from a bank. Never provide identity proof to anyone without a genuine reason, never click on any line in any email to access bank's site, access your bank website only by typing the URL in address bar of the browser, avoid using other's laptop or systems for net banking, change your password/pin often and do not make it a practice of allowing your browser to remember your userid's and passwords. Remember that banks are not authorised to ask for any details over phone, email or text.

---

[*] **https://economictimes.indiatimes.com/wealth/save/when-trouble-comes-calling-and-empties-your-bank-account**/articleshow/62504707.cms

Artificial Intelligence (AI) in auditing

The 21st century has been a fast changing world. The way we interact and transact has undergone a sea change. At the heart of the change is artificial intelligence (AI), an omnibus term that I use for a thinking machine. It can read and grasp reams of data; determine patterns and spot outliers. Unlike automation, it learns from mistakes and, like human beings, it becomes better with practice. The rise of AI is set to transform accounting, and its first cousin — auditing.

Risk assessment is critical in an audit. When auditors determine a risk strategy, they base it on knowledge obtained in similar audits. AI provides auditors information on what fellow auditors have done for a similar industry and client size.

For several decades, auditors set tone e by sampling in their attempts to tackle extensive data. They started with guesstimates, and then moved to both stratified and random sampling. Today, automation helps us to audit the entire population and not just the sample. AI has made reasonable assurance irrelevant because you can analyze the whole ledger, identify anomalies based on risk, and lay down materiality limits. Yes, sampling is a dying art and is now a pre-2020 tool.

Procurement is often replete with paperwork and multiple file formats. AI can track multiple suppliers simultaneously, and an API (application programming interface) can process unstructured data.AI helps identify which debtors are likely to default. AI-based tools evaluate debtors, investments, and suppliers, and thus determine both the accounting treatment and provisioning. Machine learning algorithms improve estimates of bad debts, write-off of stocks, and estimates of warranties.

Major CPSEs have adopted radio frequency identification (RFID), and can now improve the way they cost products, value inventory, and verify stock. Costs associated with each inventory item can now be stored, so accountants can shift from the assumptive LIFO (last in, first out) and FIFO (first in, first out) method to 'specific identification' of cost flows.

AI helps pin down anomalies such as 'warehouse-size vs inventory size', and 'inventory vs sales data correlation. With RFID tags, physical verification will be very-fast. It can track the movement of assets and the current location of fixed assets. Where transceivers are inbuilt,

tabulation is automatic. In coal and other mining companies, drones are being used in stock count. Manual stocktaking is slowly heading to obsolescence.

AI is already impacting account through automating entries. Accounting process automation has simplified data entry. In near future with NLP (natural language processing), it can 'in minutes' scan invoices, vouchers, and bank statements into accounting transactions under appropriate heads. The audit would then be on evaluating the rules rather than the transactions. AI can perform compliance analyses for 100 *percent* of transactions. This is used to segregate business expenditure.

Text processing analytics combined with natural language processing makes it easy to analyse unstructured data such as agreements, contracts, emails, and PDF files. It can identify relevant information for testing. Contract review, revenue recognition, accounting treatment of lease agreements, invoices, and purchase review are some of the areas where this technique can be effectively applied.

Income computation on investments, physical verification of investment, and balance confirmation will be taken over by AI. Payment processing, queuing up for payment based on cash flow, and provision for warranties are areas that will receive help from AI. It can speed up quarterly closing and annual audit. Consolidation becomes easier.

Will AI replace accountants and auditors? Most of the traditional audit processes will disappear. With the rise of artificial intelligence, auditors who can work effectively at the human-machine interface will be in demand. These auditors will help in the AI process, check that it works well. In the near future, auditors will be interacting more and more with computers and AI for speedier and faster audits.

E-Invoicing under Goods & Services Tax

Goods & Services Tax: The Country witnessed one of the major indirect reforms in the form of introduction of Goods & Services Tax (GST) which came into effect from 1 July 2017. This new tax administration system is evolved on the principle of one nation, one tax by bringing under its purview multiple indirect taxes that existed earlier. Among other taxes, GST has subsumed Excise Duty and Service Tax which are the two major source of revenue for the Central Government and Sales Tax/VAT/Entry Tax which are the major sources of revenue for the various state governments. The entire process of GST, i.e. from registration to filing of returns is made 'Online'.   Tax payers do not have to run from pillar to post to get different registrations such as VAT, Excise, and Service Tax.

E-way Bill (EWB): GST Council, the apex decision making body for GST has been bringing one reform after another under GST in line with the 'Digital India' initiative of the Government of India. This was followed by introduction of a uniform E-Way bill system across the country w.e.f. February 2018. This system removed the ills of the erstwhile way bill system (different e-way bills in different states) which was a major contributor to the bottlenecks at the check posts throughout the country. Since its inception in February 2018, around 60 crore E-way bills have been generated by the business organisations in the country.

E-Invoicing: The other major reform relating to GST is E-Invoicing, also known as 'Electronic Invoicing' is an electronic authentication mechanism under GST. The GST Council, in its meeting held in September 2019 approved introduction of E-invoicing in GST in a phased manner from October 2020 onwards.

At present business enterprises use an accounting/billing software or an ERP solution to create invoices (bills) and account the same in their books. Under E-invoicing, tax payers will continue to create their GST invoices on their own accounting/billing/ERP system but these invoices need to be registered with the Invoice Registration Portal (IRP) of GST Network and obtain a unique identification number for every invoice called 'Invoice Reference Number (IRN)'. Along with IRN, the IRP will also generate a digitally signed QR code containing details of the invoice. Business firms have to re-configure their accounting software/ERP system to communicate with this portal for generating IRN. Once an IRN is generated and invoice has been authenticated, its details shall be made available on the GST portal and EWB portal in real-time. Then the invoice (with QR code) can be issued to the receiver.

A GST invoice will be valid only with a valid IRN. Because of the standard e-invoice scheme (form no.INV-01), it facilitates exchange of the invoice document (structured invoice data) between a supplier and a buyer in an integrated electronic format. To sum up, 'E-invoicing' means reporting details of specified GST documents such as invoices, debit notes and credit notes to the notified

Government portal and obtaining a reference number. It does not mean generation of invoices by the Government portal. This generation of E-invoicing is made possible through various modes, e.g. Web based, application Process Interface (API) based, SMS based, Mobile app based, Offline tool based and GSP based.

Applicability: Tax payers whose aggregate turnover (based on PAN) in any preceding financial year (since 2017-18) exceeds the prescribed limit (as per relevant notification), are required to generate E-invoices. 'E-invoicing' is required for business to business (B2B) and export invoices. In the first phase, business units with turnover more than Rs.500 crore (in any of the 3 preceding financial years) shall issue E-invoices from 1 October 2020. In the second phase, business units with turnover greater than Rs.100 crore (in any of the 3 preceding financial years) hall issue e-invoices from 1 January 2021. In the third phase, business units with turnover more than Rs.50 crore (in any of the 3 preceding financial years) shall issue E-invoices from 1 April 2021. Wherever applicable, an invoice issued without obtaining IRN is not considered an invoice at all.
Exemption: Certain classes of registered persons under GST, viz. SEZ Units, Insurance, banking companies (including NBFCs), goods transport agencies, passenger transport services & multiplex cinema admissions are exempt from issuing E-invoices.

Penal provision for non-compliance: Non-generation of E-invoice is an offence and attracts heavy penal provisions up to Rs.10000 per invoice each act (CGST/SGST). Further, incorrect invoicing can lead to a penalty of Rs.25000 per invoice. If a tax payer delays generation of E-invoice, its GST returns will not get auto-populated and its customers will not be able to claim valid input tax credit.

Applicability: Tax payers whose aggregate turnover (based on PAN) in any preceding financial year (since 2017-18) exceeding the prescribed limit (as per relevant notification) are required to generate E-invoices. 'E-invoicing' is required for business to business (B2B) and export invoices. In the first phase, business units with turnover more than Rs.500 crore shall issue E-invoices from 1 October 2020. In the second phase, business units with turnover greater than Rs.100 crore shall issue e-invoices from 1 January 202. In the third phase, business units with turnover more than Rs.50 crore shall issue E-invoices from 1 April 2021. Wherever applicable, an invoice issued without obtaining IRN is considered as an invoice at all.

Exemption: Certain classes of registered persons under GST, viz. SEZ Units, Insurance, banking companies (including NBFCs), goods transport agencies, passenger transport services & multiplex cinema admissions are exempt from issuing E-invoices.

Penal provision for non-compliance: Non-generation of E-invoice is an offence and attracts heavy penal provisions up to Rs.10000 per invoice. Further incorrect invoicing can lead to a penalty of Rs.25000 per invoice. If a tax payer delays generation of E-invoice, its GST returns will not get auto-populated and its customers will not be able to claim valid input tax credit.

Expected benefits: As huge amount of real-time data is available with the Government, it is expected to curb the menace of fake invoices resulting in genuine input tax credit (ITC) claim by the tax payers. Since the invoice particulars loaded by the supplier are authenticated in the Government website, it would also enable the buyer to verify the genuineness of its supplier through automated systems. The buyer's insistence will compel suppliers to mandatorily issue e-invoice and ensure that the tax for the same is deposited with the Government. This is expected to bring down the dubious and fraudulent ITC claims by the businesses which is not only expected to help control tax evasion/plug revenue leak but bring in stronger audit trails too.

The 'On-line' saga

Thanks to the Pandemic.

The classrooms have disappeared and in come the gadget and the Internet.

Gone are the days when the facial expressions and the body language of the participants indicated their presence or otherwise in the class room.   No expressions, no body language, only the chat box, if and when activated, indicates the presence of the participants. Earlier, Chatting was something done to pass time with informal conversations (popularly known as gossip), but today with the classes going on-line, Chatting is serious business. It is the lifeline connecting the presenter with the participants.

Well, with the whole world going on-line, RTIs are no exception.

I was skeptical when our RTI went on-line and I was asked to handle a session. Though people around me had their own take on my idiosyncrasies (an euphemism for idiotic actions), I never thought that I would be required to converse with idiot boxes for hours on end !!!

But to my surprise, the **box** (of course the chat and not the idiot) responded positively right from the word go and I was bombarded with responses from even those who have not spoken a word in a full class room session for over two hours.

This experience set my think tank (Is there one !!!???!!!) rolling to analyse participant behaviour in classrooms vis-à-vis on-line sessions. How is it that participants are ready to engage themselves better when on remote and not when on-site? Is it because they do not want to embarrass themselves in front of others for wrong/irrelevant questions? Is it due to the fact that some participant was first in raising a question or responding which another participant wanted to raise or respond to? Whereas in the chat box one never knows what the other participant is thinking or keying in.

The reasons for such responses could be other than those listed above or a combination of several of these, and more.   Drawing a similarity to Sunil Gavaskar's oft-repeated statement, "one should not bother about how they (runs) come, as long as they (runs) come", an experienced presenter shouldn't bother how the responses from the participants come as long as they keep coming in. So let's not go deep into these reasons and move on to the other experiences which we have had in on-line trainings, both from the participants' as well as the presenter's perspective.

Experienced presenters maintain good eye-contact with the participants and this enables them to understand each participant's take on the proceedings, but the online mode makes it possible for the participants even to be away (without logging out) from the proceedings.   But the huge responses in the chat box indicated the keen interest of the participants even in the online mode

encouraging the co-ordinators of the training programmes and the presenters as well.

It's not only these encouraging observations that make online sessions interesting, but also their humorous side, as participants attending sessions from home inadvertently switch on their cameras/microphones. Be it their attire, animated conversations, or arguments with spouse/children while seeking assistance to sort out gadget/network related issues all the presenters have had their bags full of bloopers from the participants. The most annoying, (should I say interesting !?!) part is the logging off when a question is put across to a specific participant, with poor connectivity becoming the scapegoat.

Online sessions save a lot of time and effort for the participants, as most of them attend the trainings from the comfort of their homes.

Well, with online sessions here to stay for some more time to come with the pandemic picking up steam in its second wave, let's see the best side of it and

ENJOY

One IAAD One System

Introduction:

The purpose of the One IA&AD One system(OIOS) project is to create an IT based platform, which will create a single source of truth regarding audit activities of IA&AD. IA&AD has seen several IT applications that catered to the needs of one or more offices/audit streams in this regard. This IT application is being designed in such a way that it can be configured and used by any audit office (any audit stream and any type of audit) in the IA&AD, and also be configurable to implement future changes in audit processes, products etc.

OIOS vision

Vision Statement

To make our audit more effective by empowering IA&AD officials from the audit team upwards, and to make our audit processes more efficient and effective through a state of the art end-to-end IT solution, with seamless integration and process workflow.

Fundamental principles:

The fundamental principles governing the change management from OIOS are the following.

- OIOS will be the single source of truth regarding the envisaged activities.
- The activity or process itself must be captured in OIOS thus avoiding post-facto data entry to the maximum possible extent.
- OIOS should aim to capture the common minimum/ mandatory audit process across various offices and provide scope for office-wise configuration.

Brief about OIOS
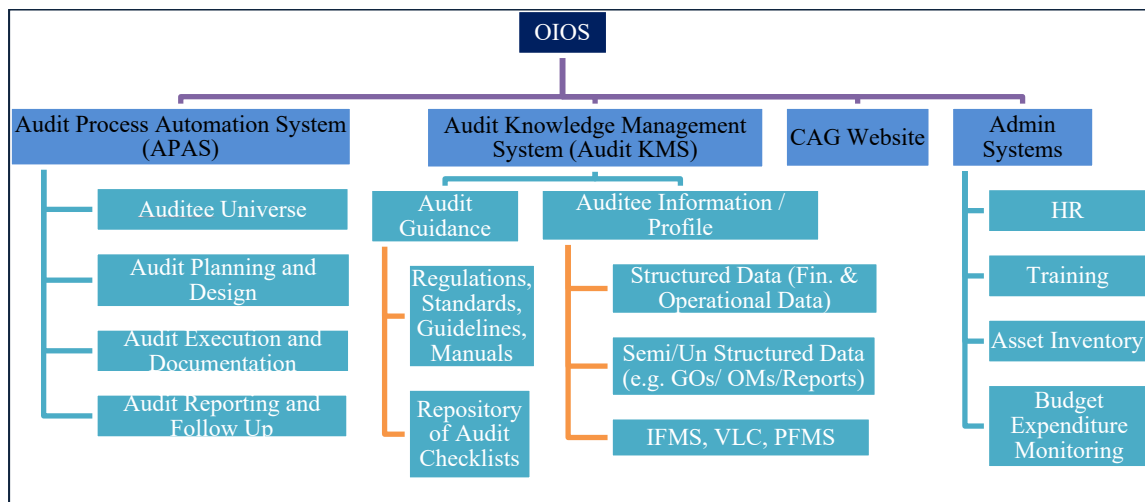
Audit Process Audit Automation System:

- Primary system of record (Single Source of Truth) for the entire chain of audit activities
    - From audit planning and design through audit execution to issue and follow-up of Inspection Reports to processing and finalisation of CAG's Audit Reports and other Audit Products
    - Activities through the IT system, workflow-based; not post facto recording
- Will ensure consistent, reliable data in a uniform format across all Audit Offices
- Dispense with numerous monthly/ quarterly returns – internal to Field Audit Office (FAO) and to CAG's office
- Supports better and real-time monitoring of the audit processes, especially audit execution
- Integration/ linkage with HR and Training systems
- Integrated with Audit Knowledge Management System
- Primary system of record for all audit processes
    - Maintaining the Auditee Universe
    - Online preparation of Audit Requisitions and Audit Observations
    - Online preparation/ processing of Inspection Reports, Departmental Appreciation Notes, Draft Performance Audits
        - Uploading of supporting documentation
    - Processing and finalization of CAG's Audit Reports
    - Follow-up of Inspection Reports, Explanatory Notes and Action Taken Reports
    - Will cover all types of audit – Compliance, Performance, Financial audit

Audit Knowledge Management System (Audit KMS)

- Audit Guidance
    - Regulations; Auditing Standards
    - Auditing Guidelines; Guidance Notes; Practice Guides
    - Manuals and Subsidiary Instructions (CAG's Office and Field Offices)
    - Repository of audit checklists
        - For adapting and re-use, as appropriate, by different Field Audit Offices
- Auditee Information
    - Will not be uniform; will vary across audit offices/ audit streams
        - Semi/ unstructured information (e.g. GOs/ GRs; Budget papers; Annual/ longer term Plans; DPRs; Procurement Documentation; Evaluation Reports)
    - Continuously growing/ updating; will need strong moderating (centrally and locally) to maintain documentation relevance

BI Reporting (Oracle Analytics Server)

- Ability to create reports and dashboards
- Supports both self-service reporting and managed service reporting
- Ability to generate documents based on templates
  - Intimation letter;
  - Draft Inspection report

Modular Approach

Phase I of the project covers the following features.

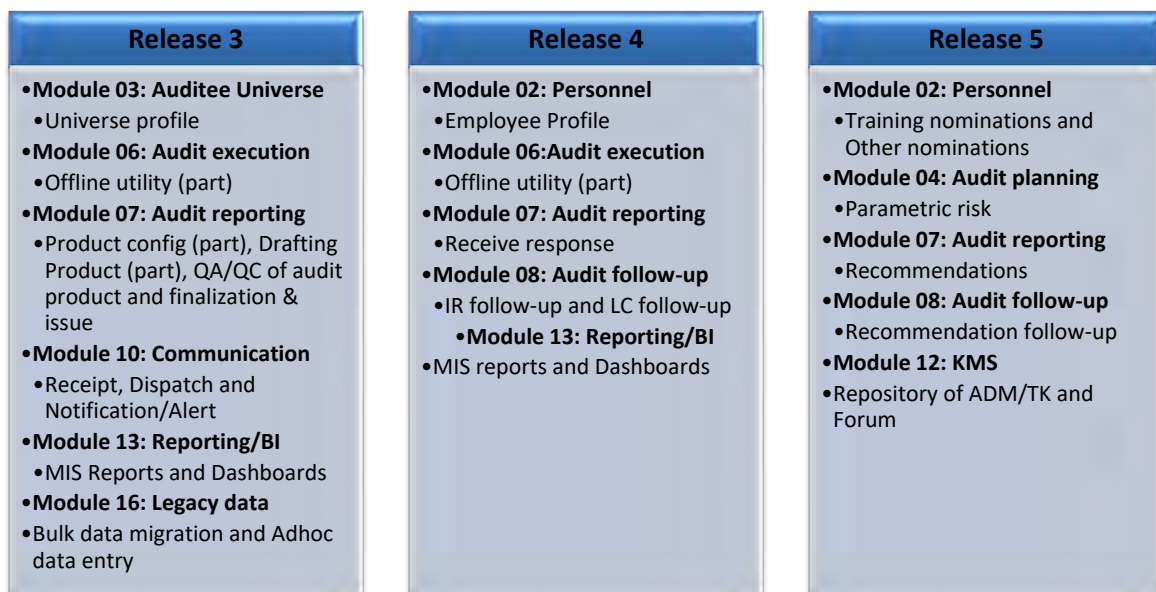| Release 1	Release 2

• **Module 01: Organisation**
  • Office master, Office structure, User privilege master, User roles and Role-structure map
• **Module 02: Personnel**
  • Employee master and Posting/transfer
• **Module 03: Auditee universe**
  • Universe master
• **Module 06: Audit execution**
  • Audit toolkit (Collect) platform (part)
• **Module 09: Data collection**
  • Design kit, Allocate access, Monitor collection and Consolidate and analyse
• **Module 12: Knowledge management system**
  • Audit guidance (part) and Auditee IS (part)
	• **Module 02: Personnel**
	  • Gradation list
	• **Module 04: Audit Planning**
	  • Annual Audit Plan
	• **Module 05: Audit design**
	  • Audit design matrix, Sampling approach and Audit guidelines
	• **Module 06: Audit execution**
	  • Programme, Record requisition, Audit enquiry, Audit observation and Audit toolkit (collect) platform (part)
	• **Module 07: Audit reporting**
	  • Product configuration (part) and Drafting **product** (part)
	• **Module 12: Knowledge management system**
	  • Audit guidance (part) and Auditee IS(part)
	• **Module 13: Reporting / Business Intelligence**
	  • MIS reports and Dashboards

Phase II covers the following features

Release 3	Release 4	Release 5

• **Module 03: Auditee Universe**
  • Universe profile
• **Module 06: Audit execution**
  • Offline utility (part)
• **Module 07: Audit reporting**
  • Product config (part), Drafting Product (part), QA/QC of audit product and finalization & issue
• **Module 10: Communication**
  • Receipt, Dispatch and Notification/Alert
• **Module 13: Reporting/BI**
  • MIS Reports and Dashboards
• **Module 16: Legacy data**
• Bulk data migration and Adhoc data entry
	• **Module 02: Personnel**
	  • Employee Profile
	• **Module 06:Audit execution**
	  • Offline utility (part)
	• **Module 07: Audit reporting**
	  • Receive response
	• **Module 08: Audit follow-up**
	  • IR follow-up and LC follow-up
	    • **Module 13: Reporting/BI**
	• MIS reports and Dashboards
		• **Module 02: Personnel**
		  • Training nominations and Other nominations
		• **Module 04: Audit planning**
		  • Parametric risk
		• **Module 07: Audit reporting**
		  • Recommendations
		• **Module 08: Audit follow-up**
		  • Recommendation follow-up
		• **Module 12: KMS**
		• Repository of ADM/TK and Forum

Activity:

Phase I soft launch in six pilot offices was on 26th July 2020. Among the user offices under RTI, Chennai, Office of the AG(Audit)II, including Puducherry Branch office were the pilot offices for soft launch.

Implementation of OIOS includes

Management of master data (organization, employee and auditee universe)

As a Coordinator, RTI, Chennai, supported the AG (Audit)II Office Administrators and Wing Administrators in capturing the above data. Validation and Data cleaning as per the requirements for OIOS, Testing the Bulk uploading in UAT environment.

Workshop was conducted during August and September 2020, to the user office (AG Audit II, Tamilnadu) including Branch office Puducherry. The following sessions were covered;

Session 1: Creation of employee accounts
Session 2: Creation of posts and posting of employee

Session 3 & 4: Audit planning
 • Creation of Annual audit plan for 2020-21
 • Addition of assignments taken up for 2020-21
 • Prepare design of the assignments
    • Map auditee entities
    • Prepare sampling approach (if relevant)
    • Prepare audit design matrix

Session 5: Audit execution:
    • Create audit teams
       • Create audit programme

Session 6: Field visit demo and training
    • Record requisitions
    • Audit enquiry
    • Audit observation

Session 7: Field visit demo and training
    • Fill ADM
    • Digital diary
    • Deviation request
    • Generate draft IR

Session 8 & 9: Data collection toolkit
    • Designing questions (workflow, translation)
    • Collection
    • Monitoring responses

Session 10: Auditee Information System and Audit Guidance
Session 11: Maintain auditee universe and searches
Session 12: Publishing ADM in central repository and reuse
Session 13: Publishing Toolkit in central repository and reuse

Roll-out to 32 nodal offices covering 66 offices including Branch offices was taken up during September 2020.

Out of 66 nodal offices, the following are the user offices under RTI Chennai.

1	Office of the AG(Audit-I), Kerala
2	Office of the AG(Audit-II), Kerala
3	Branch: PAG (Audit-I), Kerala
4	Branch: PAG (Audit-II), Kerala
5	Office of the AG(Audit-I), Tamil Nadu
6	DGA (Central), Chennai
7	Branch: DGA (Central), Kochi
8	Branch: F&C Audit, Chennai
9	Branch: F&C Audit, Thiruvananthapuram

As of now, the support is being extended to the above offices for capturing the master data.

Further, the workshop on various modules for the above offices were being completed during February/March 2021.

The environment and the human species

We are constantly worried about the environment. Most of us live in cities where pollution levels are insanely high, there is decreasing green cover, and every year during summer months there is water shortage. The seas are getting depleted of its resources. Land is turning fallow with overuse. The worst part of the problem is that we know it is only going to get worse. The carbon levels are not going to come down. Species gone extinct are lost forever. Our development paradigm is linked hopelessly with a course that leads us minute-by-minute to greater and greater destruction. We perceive and measure development in terms of roads built, resources utilized, better purchasing power for the people and greater consumption. But the resources available to us is very limited, and the more we consume, the dearer the remaining stock become. Our ideals of improved living and sustainable living are, strangely, at odds with each other and there is not a sign of truce anywhere in sight.

How did we turn into such an over-consuming, over-breeding, invasive species that lives and wallows in its own waste? Where exactly did we go wrong? How far back should we go if we were to decide on a course correction? The renowned American scientist and author of many books on popular science, Jared Diamond, in an essay published in the Discover Magazine, posits that the adoption of agriculture was possibly the 'worst mistake in the history of the human race' that irreversibly set us on a course of rapid increase in numbers, large scale exploitation of natural resources, and lead us to the present predicament of ecological disaster.

The human species, which possibly came into existence about one lakh years ago, started on agriculture very late, only by the last one tenth of its existence, when our ancestors, at various corners of the inhabited world, started domesticating plants and animals. Before that all humans were hunter gatherers, catching wild animals and foraging for edible parts of plants. And then, after existing thus for almost 9 millennia, almost as if by magic, we stumbled upon this new trick of growing crops. The advantages were obvious. Agriculture left us with a huge surplus. Whereas finding food was what occupied a hunter gather for most of his waking hours, the trick of mass producing seeds which can be stored away and used for food whenever needed left mankind with a lot of time on its hands, to create the great works of art and literature, to organize into nations, to invent science and to engage in philosophy. Apparently we are much better off than our hunter-gatherer forefathers. We have more leisure, more security, and more chances of living a longer, happier life.

But recent archaeological and anthropological observations do not support these popular notions of the supposed advantages of our modern agrarian societies. There still exist, scattered throughout the planet, communities of primitive people, who still lead the lives of hunter-gatherers. Do they spend all their time

finding food? Observations of these people reveal a surprising fact. They are more relaxed, they play more and sleep more and work much less hard than an average city dweller.

Agriculture restricted us to a woefully limited diet of a few starchy plants like rice, wheat and potatoes. The pre-agrarian people on the other hand diet on a wider range of wild plants and animals providing them with a better balance of proteins, fibre and other nutrients. "It's almost inconceivable", says Jared Diamond, "that Bushmen of Kalahari, who eat 75 or so wild plants, could die of starvation the way hundreds of thousands of Irish farmers and their families did during the potato famine of the 1840s."

Yet, with agriculture, it was possible to feed a larger population and hence, like any natural species, we started increasing in numbers. With agriculture also came the notion of ownership of land and property. For a hunter, there was no advantage in holding on to an area of hunting ground, for his prey roamed wild. For a farmer, on the other hand, it was necessary to preserve his land and guard it from intrusions. Agriculture also gave rise to deep class divisions, because the surplus permitted classes of people to parasitize and grow fat on the food produced by another class of humans. When the land progressively lost its fertility, it became necessary to cultivate larger tracts and expand to marginal lands to support the existing population. This necessitated that the original inhabitants of these lands, the wild animals and plants, be driven out and restricted to smaller and smaller spaces. In time this desperate expansion got rationalized in popular imagination as 'enterprise' and, linked to survival, became an essential human value. Need became indistinguishable from greed, and this drama of hungry hoards raiding a land played out in myriad theatres around the world, in Africa and the Americas as conflict between the natives and the invading Europeans, and elsewhere as colonialist exploitation.

We developed technology so that extraction of resources kept pace with the growing demand and we resorted to boosting demand, engineering need, even, to support the production. We created social values that glorifies ambition and venerates affluence. We created social institutions that train and support humans to become able handlers of this technology. We exist in an economic, political, ethical and psychological milieu that drives us blindly towards consuming more, and revealing and taking pride in our consumption. We may need more than just lamentations and occasional seminars to see us through this conundrum, to be more than just bad custodians of our children's property.

Web browsing with Family

When you and your family surf the Web it's important to keep the following in mind:

- Online information is usually not private.

- People online are not always who they say they are.

- Anyone can put information online.

- You can't trust everything you read online.

- You and your family may unexpectedly and unintentionally find material on the Web that is offensive, pornographic (including child pornography), obscene, violent, or racist.

Step 1: Secure your home Wi-Fi network.

Step 2: Consider common place for computer to children and family

Step 3: Set family rules for accessing internet

Step 4: Understand the need and set boundaries for online safety

Step 5: Use Parental Controls

Step 6: Secure your computer

Step 7: Keep your software up to date

Step 8: Install Antivirus, Desktop Firewall solutions against malware and unauthorized access

Step 9: Back up your system

Step 10: Use separate standard user accounts for family members

Step 11: Create strong and easy to remember passwords for your accounts.

Step 12: Secure your web browser before accessing the internet

Step 13: Be careful online and don't click suspicious links

Step 14: Ensure safe browsing for everyone, even for grandparents!

Step 15: Download and install software from trusted sources only.

Tips and Best Practices for Safer Social Networking

Social media have become an important part of our life. We share updates with our friends, family and anyone who is concerned using social media. But hackers can use this information to steal sensitive data and hack your account. Given below are some of the general tips on using social media.

- Always ask the questions:
  - Who can access the information I am putting online?
  - Who controls and owns the information I put into a social networking site?
  - What information about me are my contacts passing on to other people?
  - Will my contacts mind if I share information about them with other people?
  - Do I trust everyone with whom I'm connected?
- Always make sure you use secure passwords to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine.
- Make sure you understand the default privacy settings offered by the social networking site, and how to change them.
- Consider using separate accounts/identities, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. Delete your password and browsing history when using a browser on a public machine.
- Access social networking sites using **https://** to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.
- Be careful about putting too much information into your status updates – even if you trust the people in your networks. It is easy for someone to copy your information.
- Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly careful when integrating your social network accounts! You may be anonymous on one site, but exposed when using another.
- Be cautious about how safe your content is on a social networking site. Never rely on a social networking site as a primary host for your content or information. It is very easy for governments to block access to a social

networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

Posting Personal Details

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. Perhaps the biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common. In addition, the more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities. The online activities of diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands.
Ask yourself: is it necessary to post the following information online?

- birth dates
- contact phone numbers
- addresses
- details of family members
- sexual orientation
- education and employment history

Friends, Followers and Contacts

The first thing you will do after filling in your personal details with any social networking application is establish connections to other people. Presumably these contacts are people you know and trust – but you may also be connecting to an online community of like-minded individuals that you have never met. The most important thing to understand is what information you are allowing this online community to have.

When using a social network account such as Facebook, where a lot of information about yourself is held, consider only connecting to people you know and trust not to misuse the information you post.

Status Updates

On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening? The most important thing to understand about the status update is who can actually see it. The default setting for the status update on most social networking applications is that anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

To do this in Twitter, look for "Protect Your Tweets". In Facebook, change your settings to share your updates with "Friends Only". Even if you switch to those settings, consider how easy it is for your information to be reposted by followers and friends. Agree with your network of friends on a common approach to passing on the information posted in your social networking accounts. You should also think about what you may be revealing about your friends that they may not want other people to know; it's important to be sensitive about this, and to ask others to be sensitive about what they reveal about you.

There have been many incidents in which information included in status updates has been used against people. Teachers in the US have been fired after posting updates about how they felt about their students; other employees have lost their jobs for posting about their employers. This is something that nearly everyone needs to be careful about.

Sharing Online Content

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have? If you share (or "like") a site that opposes some position taken by your government, for example, agents of that government may take an interest and target you for additional surveillance or direct persecution.

If you want your contacts (and of course the administrators of the social networking platform you use) to be the only ones who can see the things you share or mark as interesting, be sure to check your privacy settings.

Revealing your Location

Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safe about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

Sharing Videos and Photos

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

Instant Chats

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

Connecting to the site via https is a minimum requirement for secure chatting, but even this is not always a guarantee that your chat is using a secure connection. For example, Facebook chat uses a different channel to HTTPS (and is more prone to exposure). It is more secure to use a specific application for your chats, such as Pidgin with an off-the-record plugin, which uses encryption. Read the 'Pidgin – secure instant messaging' hands-on guide.

Joining and Creating Groups, Events and Communities

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

When you join a community or group online it is revealing something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups, for example. Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so? For example, perhaps it is a gay and lesbian support group that you have set up to help people, but by joining it people are openly identifying themselves as gay or gay-friendly, which could bring about dangers for them in the real world.

Unified Payment Interface(UPI)-How it works?

Unified Payment Interface (UPI) is an initiative by National Payments Corporation of India (NPCI), set up with the support of the Reserve Bank of India with a vision of migrating towards a "less-cash" and more digital society.

UPI is a system that enables peer to peer online payments for users holding different bank accounts, to send and receive money or to pay directly to merchants from their smartphone without the need to enter bank account information or net banking UserID / Password.

UPI is built on the Immediate Payment Service (IMPS) platform.

How it works

For using Unified Payment Interface, users need to create a Virtual ID or Virtual Payment Address (VPA) of their choice to link it to any bank account. This process doesn't require either the payee or payer to share bank details. The VPA acts as their financial address and users need not remember beneficiary account number, IFSC codes or net banking user id/password for sending or receiving money.
Registration

Steps for Registration:

- User downloads the Unified Payment Interface application from the App Store / Banks website.
- User creates his/ her profile by entering details like name, virtual id (payment address), password etc.
- User goes to "Add/Link/Manage Bank Account" option and links the bank and account number with the virtual id.

Generating M-PIN:

- User selects the bank account from which he/she wants to initiate the transaction.
- User clicks on the given options as required.

Performing a Unified Payment Interface Transaction

PUSH-sending money using virtual address

- User logs in to UPI application.
- After successful login, user selects the option of Send Money / Payment.
- User enters beneficiary's / payee virtual id, amount and selects account to be debited.

- User gets confirmation screen to review the payment details and clicks on 'Confirm'.

- User now enters MPIN.

- User gets successful or failure message.

PULL-Requesting money

- User logs in to his bank's UPI application.

- After successful login, user selects the option of collect money (request for payment).

- User enters remitters / payers virtual id, amount and account to be credited.

- User gets confirmation screen to review the payment details and clicks on confirm.

- The payer will get the notification on his mobile for request money.

- Payer now clicks on the notification and opens his banks UPI app where he reviews payment request.

- Payer then decides to click on accept or decline.

- In case of accept payment, payer will enter MPIN to authorize the transaction.

- Transaction complete, payer gets successful or decline transaction notification.

- Payee / requester get notification and SMS from bank for credit of his bank account.

Advantages

- With UPI, user's bank account can be used as a wallet with a simplified two-factor authentication which eliminates the need to store funds in any other wallet.

- Use of Virtual ID makes it more secure since there is no need to share credentials.

- UPI transaction can be made via IMPS in real time, which makes it available 24*7.

- Users can link multiple bank accounts to a single Smartphone. Hence sending or receiving money across banks is easier.

- For merchants, it is suitable for electronic commerce and mobile commerce transactions as well as it resolves the cash on delivery collection problem.

- Banks can create their own application interfaces as UPI provides flexibility and an open architecture.

Security Measures

- Beware of mobile phishing: always download legitimate UPI applications from bank's official website, and be cautious before you download it from App store.

- Keep strong passwords for your phone as well as for your UPI application.

- Do not share MPIN with anybody (not even with bank), and be suspicious of unknown callers claiming to be from your bank.

- Use biometric authentication if possible.

- Update your mobile OS and applications as often as possible to be secure from vulnerabilities.

- It is advisable for users to enable encryption, remote wipe abilities and anti-virus software on the phone.

- Keep your SIM card locked with a Pin to avoid misuse, in case of loss or theft of the mobile device, You can contact your subscriber to block the subscription of the SIM card.

- Avoid connecting phones to unsecured wireless networks that do not need passwords to access.

---

[1] *Reference: http://www.cert-in.org.in/*

Quiz - Cyber security Initiatives in India

1. It is the integrated intelligence grid developed by C-DAC-Pune connecting databases of core security agencies of the Government of India.

   a) National Intelligence Grid (Natgrid) project of India
   b) National Critical Information Infrastructure Protection Centre (NCIPC) of India
   c) IUSCSF
   d) NISAP

2. It is a project under National e-Governance Plan(NeGP) covering all 28 States and 7 UTs which aims at creation of a nation-wide networking infrastructure for evolution of IT-enabled sophisticated tracking system around 'investigation of crime and detection of criminals'.

   a) NATGRID
   b) NCCC
   c) NCIPC
   d) CCTNS

3. It is a premier industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy.

   a) NATGRID
   b) Botnet Clearing Center
   c) Data Security Council of India (DSCI)
   d) National Crime Records Bureau (NCRB)

4 This an endeavour to empower Indian Police with Information Technology and Criminal Intelligence to enable them to effectively & efficiently enforce the law & improve public service delivery.

   a) NATGRID
   b) National Crime Records Bureau
   c) National Cyber Coordination Centre
   d) Crime and Criminal Tracking Networks and Systems

5 ._____ based exercises are focused on assessing the effectiveness of security plan, coordination and communication and Standard Operating Procedures (SOPs) of the participating organization

   a) Simulated attack
   b) Hypothetical scenario
   c) Discussion
   d) Artifact

6.In this kind of exercises, participants are provided with virtual images to protect from cyberattacks. During the drill the attacker team launch announced or un-announced attacks on the setup and try to exploit the vulnerability that was present in the drill setup hosted by the organization. The organization needs to respond to the attacks according to their security plans/ SOPs/ coordination plan. Evaluator/observer monitors the actions of the participating teams.

    a) Artifact based exercise
    b) Table top exercise
    c) Walk through exercise
    d) Real-time simulation based exercise

7. Tools such as the _____ can be used for developing master inject list, trial-run and exercise-management.

    a) MOSFET
    b) COSA
    c) EXITO
    d) CISSP

8. Who created a model framework for establishing and evaluating information security (information assurance) programs, now known as The McCumber Cube

    a) Albert McCumber
    b) John McCumber
    c) Palo Alto
    d) Mike McCumber

9. This was created for rapid identification & response to security incidents and information exchange to reduce the risk of cyber threat and resultant effects.

    a) National Cyber Alert System
    b) NATGRID
    c) National Criminal and Crime Control Center
   d) National Critical Infrastructure Cyber Security Center

10 Although technical procedures vary depending on the categorization and type of incident, each incident must include the following six (6) phases: Preparation, Detection, Containment, Remediation, Resolution and _____.

    a) Closure
    b) Penetration
    c) Reporting
    d) Recording

Answers to the Quiz

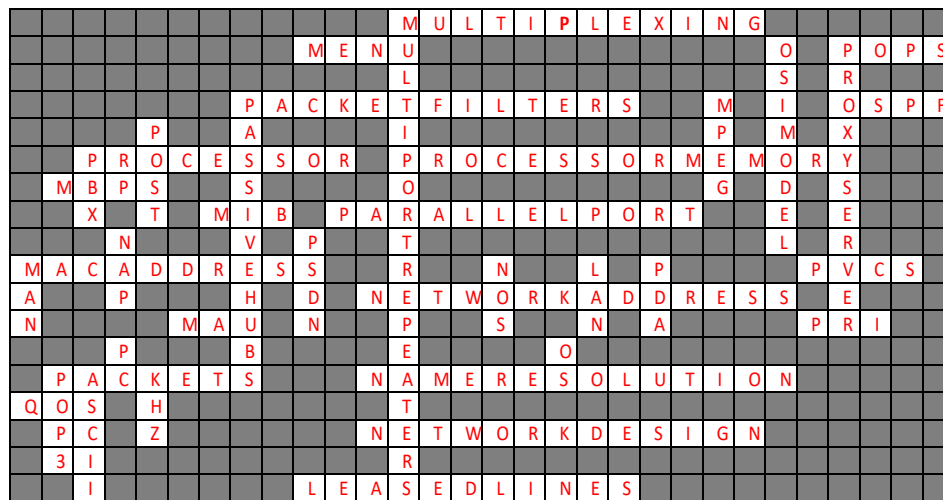(1-a , 2-d, 3-c, 4-b, 5-b, 6-d, 7-c, 8 b, 9-a, 10-a)

Crossword puzzle
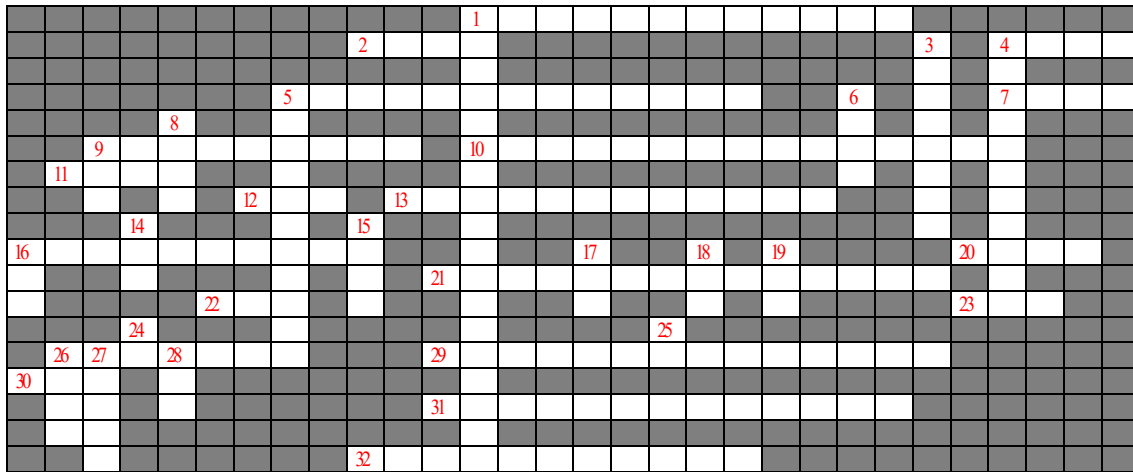
Across

1. Process of putting multiple signals on a wire simultaneously.

2. Horizontal **bar** containing the labels of drop-down **items** in an operating system's GUI. It provides the user with a standard place in a window to find the majority of a program's essential functions.

4. An artificial demarcation point or interface point between communications entities.

5. Security method that filter by IP address; not adequate security for a network.

7. A link-state hierarchical interior gateway protocol for network routing.

9. Brain of the computer system where calculations and decisions are made; also referred to as the CPU.

10. Referred to as the L1, an interface between the processor and the cache.

11. Data transfer speed.

12. A type of database used to manage the devices in a communication network.

13. Port where the bits travel down parallel paths, arriving one byte at a time; which can supply more bytes of data per unit time.

16. Unique 6-byte address associated with and coded into each network interface card (NIC)

20. Use a real, shared circuit in the service provider's backbone.

21. Part of an IP address that is uniquely assigned by one of the ICANN-sanctioned agencies.

Down

1. Allow multiple devices to be wired to a central location, share the same media, and regenerate (repeat) the signal; also referred to as active hubs.

3. The model developed to provide a view of the distinct functionalities that are required to implement each protocol layer; defines a complete range of functions that can be achieved with data communications equipment.

4. Sits between the network router and the Internet; talks to the Internet on behalf of a network's resources, allowing real network addresses to be hidden.

5. Used in a LAN environment; special form of repeater that allow multiple devices to be wired into a central location and share the same media; do not regenerate (repeat) the signal.

6. Digital video format; a working group of ISO/IEC charged with the development of video and audio encoding standards.

8. The pre-boot sequence for a computer, router, or printer.

9. A telephone exchange that serves a particular business or office.

14. Transitional data communications facilities at which Network Service Providers (NSPs) would exchange traffic, in replacement of the publicly-financed NSFNet Internet backbone; now replaced by modern IXPs.

15. A publicly available network supporting packet-switched data, separate from PSTN.

16. Connects sites in and around a large city.

22 Converts signals on an Ethernet cable to and from AUI signals.

23 An integrated services digital network (ISDN) configuration, usually intended for large users.

26 Data structures that collectively represent the transmission stream (headers and data); associated with the network layer when the communication protocol is connection-oriented.

29 Process by which the peer-to-peer name used on each conversational level is related to other levels.

30 The capability of a network to provide better service to selected network traffic over various technologies.

31 How the various clients and servers are arranged for purposes of connectivity, performance, and security.

32 Another name for private lines, dedicated lines, or permanent circuits.

17 Optimizes the client/server architecture; provides and supports network services such as file services, e-mail, Internet and intranet services, and applications.

18 Network that operates within a small geographic area, usually within a building, office, or department.

19 Hand-held computer with a touch screen.

24 A microcomputer whose price, size, and capabilities make it useful for individuals.

25 Interface between the application (word processor, spreadsheet, etc.) and the computer hardware.

26 How clients access their mailboxes on the messaging server; usually done in its third version.

27 An 8 bit is a character encoding standard

28 A unit of measurement of frequency, also known as ('000) cycles per second.

Solution

										M	U	L	T	I	**P**	L	E	X	I	N	G						
								M	E	N	U										O		P	O	P	S	
										L											S		R				
					P	A	C	K	E	T	F	I	L	T	E	R	S		M		I		O	S	P	F
			P		A					I							P		M		X					
	P	R	O	C	E	S	S	O	R		P	R	O	C	E	S	S	O	R	M	E	M	O	R	Y	
M	B	P	S		S					O							G		D		S					
	X		T		M	I	B		P	A	R	A	L	L	E	L	P	O	R	T		E		E		
	N			V		P			T										L		R					
M	A	C	A	D	D	R	E	S	S		R			N		L		P				P	V	C	S	
A		P			H		D		N	E	T	W	O	R	K	A	D	D	R	E	S	S		E		
N			M	A	U		N		P			S			N		A			P	R	I				
	P			B					E				O													
P	A	C	K	E	T	S		N	A	M	E	R	E	S	O	L	U	T	I	O	N					
Q	O	S	H					T																		
P	C	Z					N	E	T	W	O	R	K	D	E	S	I	G	N							
3	I						R																			
	I					L	E	A	S	E	D	L	I	N	E	S										

38

Training Course on Internal Controls & Internal Audit

All India Workshop on 'Goods & Services Tax' from 18.01.2021 to 22.01.2021

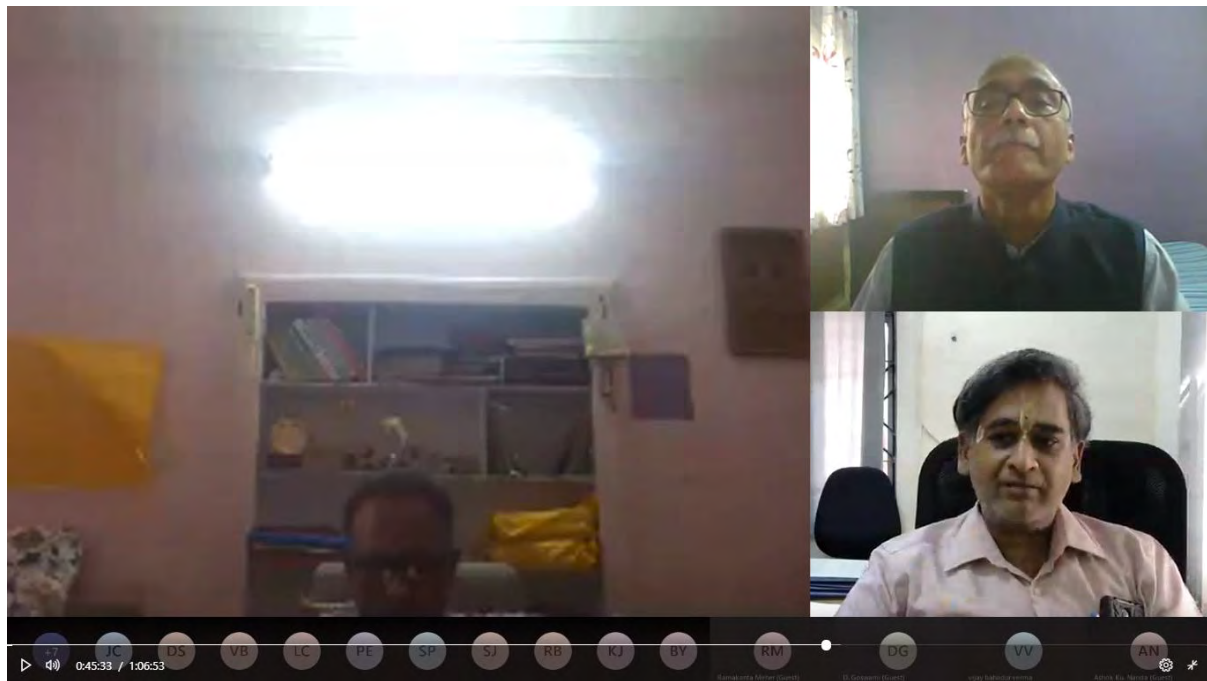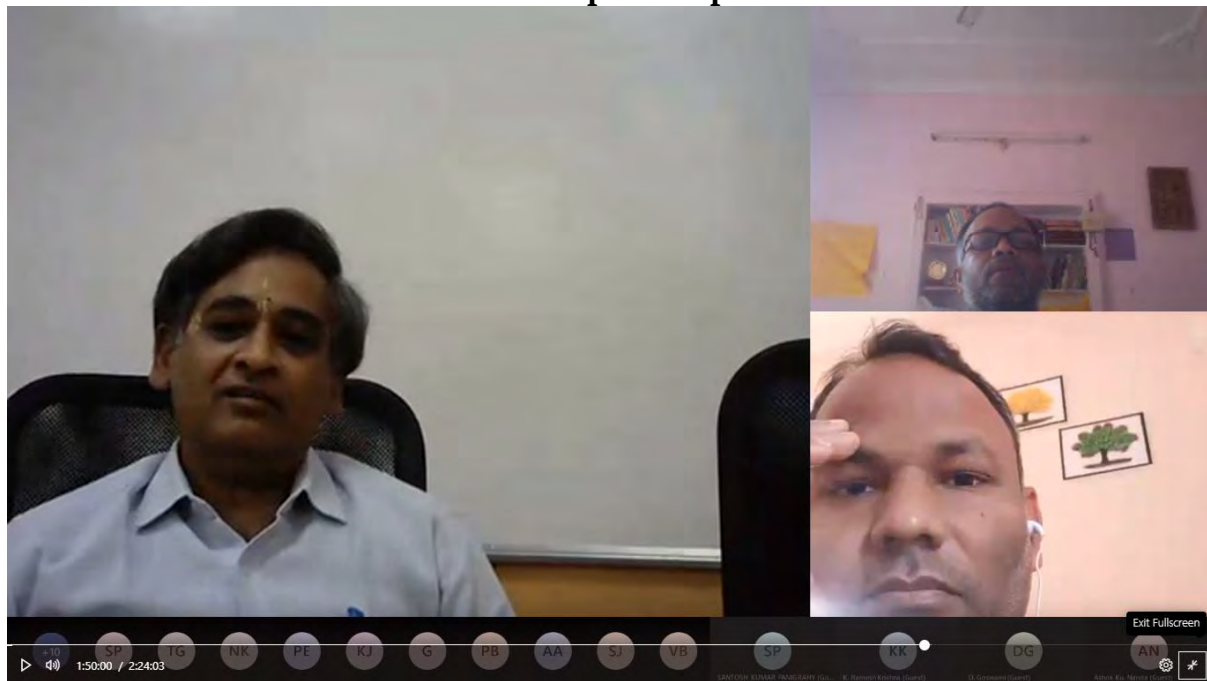**All India Workshop on 'Goods & Services Tax' from 18.01.2021 to 22.01.2021**

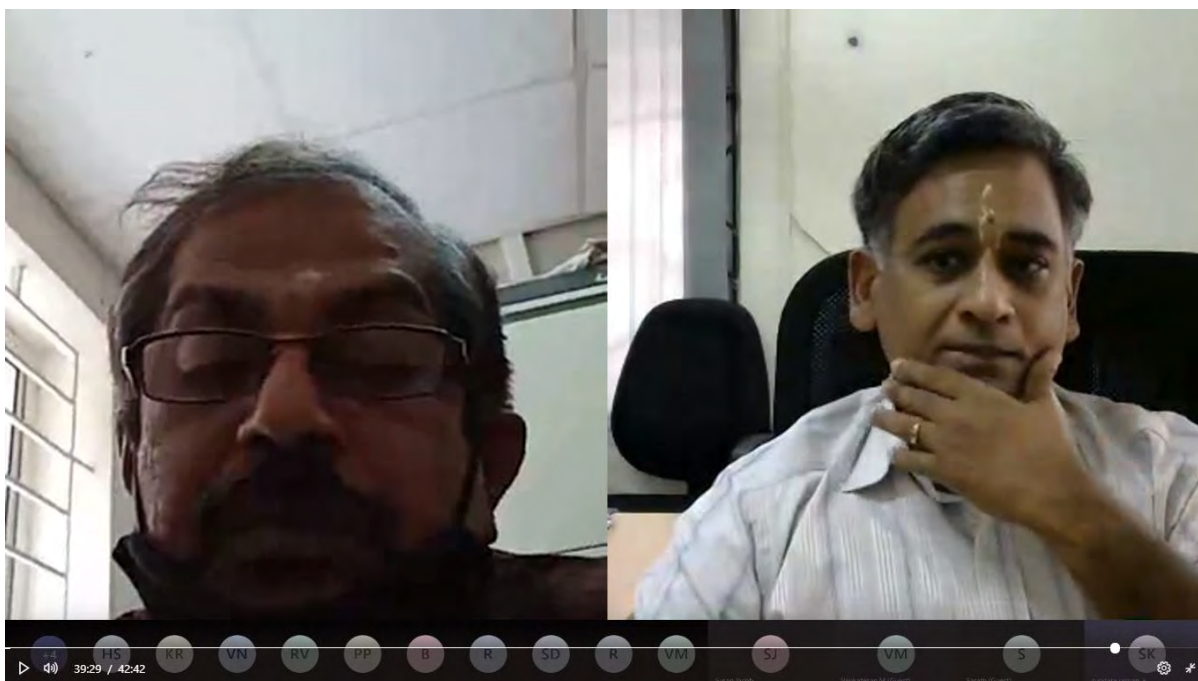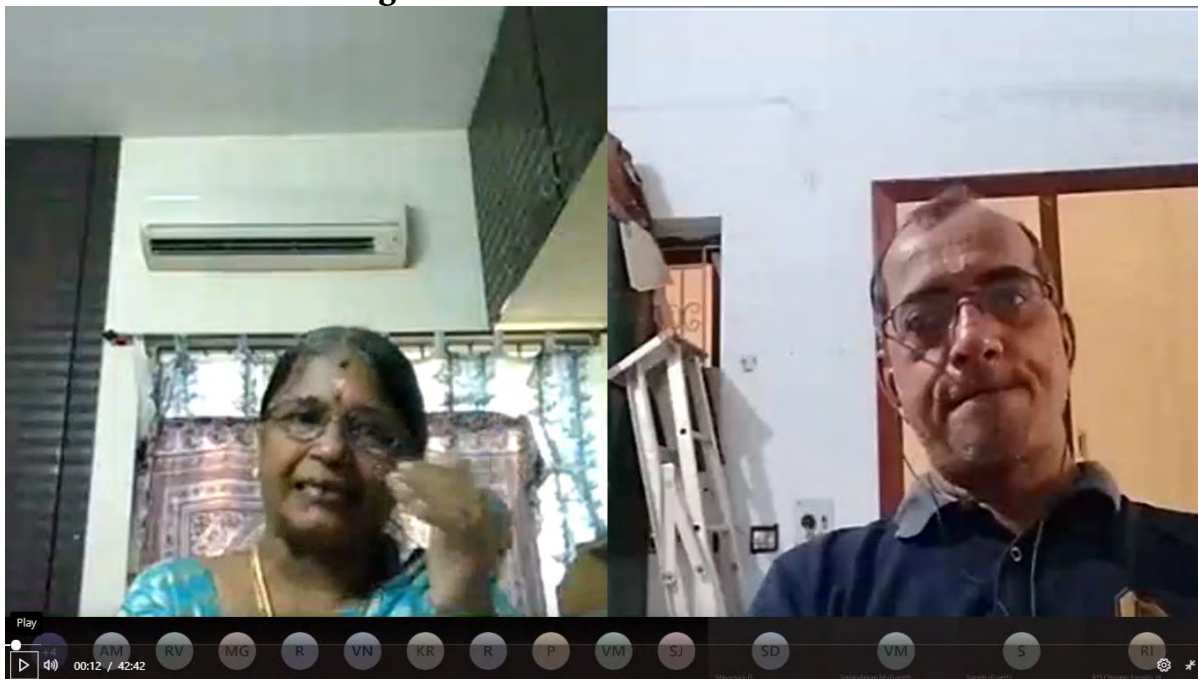**Training Course on Ind-As from 14.12.2020 to 18.12. 2020**

All India Workshop of Preparation of SFR

Training Course on 'Awareness of ISSAI'
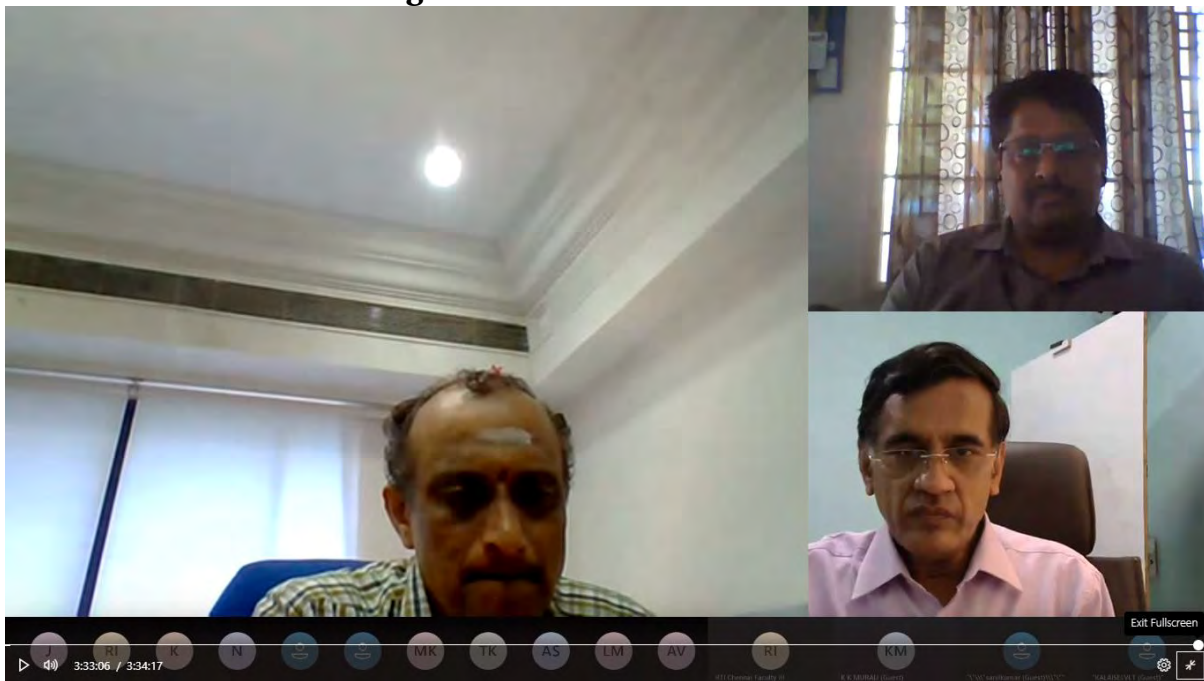
Data Analytics with Tableau 21/12/20 to 24/12/20