From Director General's Desk

Forerunner is newsletter of RTI Nagpur, which is nominated as knowledge centre for State Revenue Audit and also Central Revenue Audit (including Transfer Pricing). During the period **2008-09 to 2020-21** the institute had developed and disseminated the material on the subject of Knowledge Resource Centre as well as other topics which is available on the Institute's Web-site.

We have upgraded our infrastructure in labs and hostel besides training wing, which is hopefully will be utilized in future (when trainings would be conducted onsite). During this half yearly period (October 2020 to March 2021) we have conducted courses (online) as per Calendar of Training Programme. We have also conducted course in three batches for **Divisional Accountants** of PAG (A&E-MP)-I Gwalior in the months of October and November 2020.

In this pandemic period, we have to switch from onsite to online trainings. I take this opportunity to appreciate our faculties, participants and user offices who have adopted this new mode of training seamlessly despite many hurdles. We have also brought up interesting articles on 'Public Private Partnership– definition and characteristics, Evolution of Data Analytics, Computer security-threats and remedy, Suspense Accounts, and Overview of OIOS' in the current Newsletter.

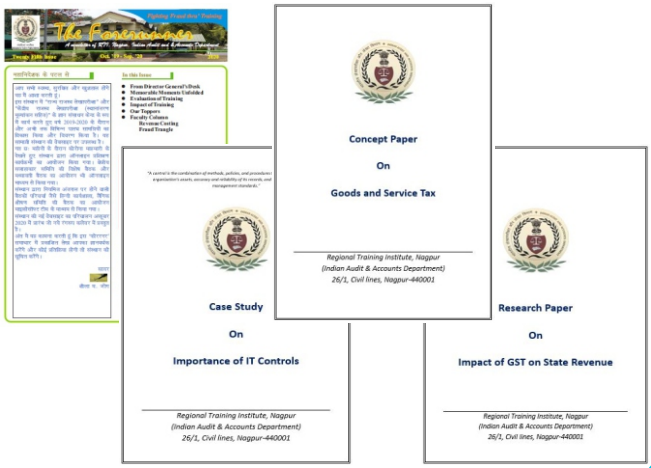
Lastly, through this newsletter, I wish to convey my sincere thanks to all officers who have attended RAC in January 2021 and provided us their valuable inputs towards the cause of strengthening RTI in each sphere. I would look forward to some more suggestions or feedback, if any, for further improvement.

Regards

Sheela M. Jog

In this Issue

Our Products



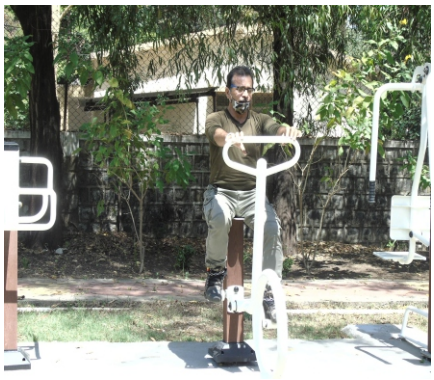
The Mandate

Headquarter has declared this institute as a Knowledge Resource Centre in 'Central Revenue Audit including Transfer Pricing' in April 2015 and 'State Revenue Audit' in May 2020 with a mandate to act as a repository of information on the subject through developing quality Reading Material, Case Studies (National and International), Research Papers and database of expert faculty and media reports. Significant development in the matter are reported through a newsletter for information to the user offices and sister Institutes.

यादगार लम्हे MEMORABLE MOMENTS UNFOLDED

Open Garden Gym Inaugurated by Ms. Heme Munivenkatappa Accountant General (Audit)-II, Nagpur on 03.03.2021

DG, RTI, Nagpur, PAG(A&E)-II, Nagpur & AG (Audit)-II, Nagpur watching demonstration of Gym equipments



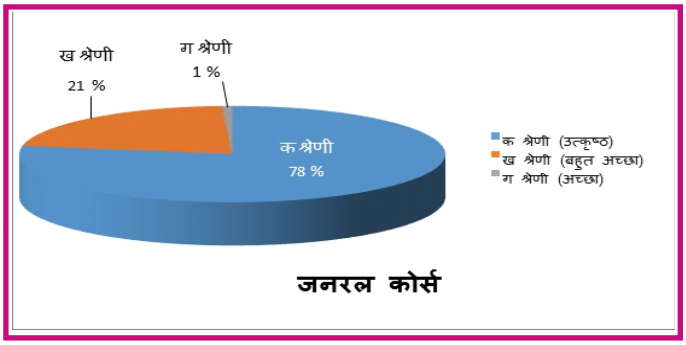
Demonstration of open Garden Gym by Trainer

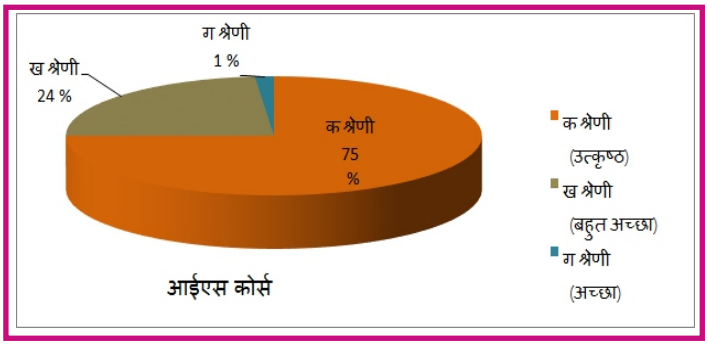
Tree plantation by Sheela M. Jog, Director General and faculty member of RTI, Nagpur

प्रशिक्षण का मूल्यांकन (EVALUATION OF TRAINING)

प्रतिभागियों की प्रतिक्रिया के आधार पर प्रत्येक प्रशिक्षण कार्यक्रम का मूल्यांकन किया जाता है एवं उस पाठ्यक्रम को ग्रेड दिया जाता है। नीचे दशाये गये चार्ट में General एवं IS Based पाठ्यक्रमों के ग्रेड को दर्शाया गया है।

अक्तुबर 2020 से मार्च 2021 के दौरान आयोजित पाठ्यक्रमों की रेटिंग





Continuing Professional Education (CPE)

(अक्तूबर 2020 से मार्च 2021 के बीच संस्थान के संकाय द्वारा प्राप्त प्रशिक्षण)

नाम	विषय	प्रशिक्षण का स्थान
श्री जी.के. ओमी, स.ले.प.अ./संकाय	Certification - "Big Data Computing" (Online Course) National Training Programme on "Big Data Analytics" (Online)	IIT, Kanpur (NPTEL) iCISA, Noida

सामग्री हेतू हमें संपर्क करें :

Contact us for material

e-mail : rtinagpur@cag.gov.in
Ph. (0712) 2545420, 2545816, 2545829
Fax : 0712 - 2562577, Hostel - 2552252
Web : https://cag.gov.in/rti/nagpur/en

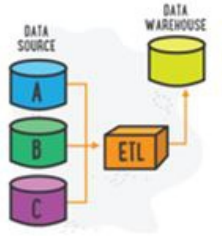
The evolution of Data Analytics

It is believed that we have lived through two eras in the use of Analytics. We might call them BBD - Before Big Data and ABD - After Big Data.

The use of data to make decision is not a new idea; it is as old as decision making itself. But the field of business analytics was born in mid-1950s with the advent of tools that could produce and capture a larger quantity of information and discern patterns in it in more quickly than the unassisted human mind ever could. The era of Analytics also referred in terms of:

Analytics 1.0: the era of "business intelligence"

It was the era of BI in 1990s where we use to deal with the pre-defined queries and descriptive or historic views of structured data. Data like sales data, financial data etc. The data was stored in traditional relational database systems where data neatly fits in rows and columns. In this era analysts spent a majority of their time in preparing data for analysis and relatively little time on the analytics itself.



Analytics 2.0: the era of "big data"

In 2000s, the era of Big data analytics with competitive insight which added complex queries along with forward-looking and predictive views leveraging both structured and unstructured data. Well! I have not told anything about unstructured data. It is data captured from social media, mobile data, call centers logs, feedbacks, reviews, complaints in the form of text. All these stuffs will comprise unstructured data.

Analytics 3.0: the era of data-enriched offerings

Today, massive amounts of data are being created at the edge of the network and the traditional ways of doing analytics is no longer viable. The data is being generated rapidly at the personal devices. Every device, shipment and consumer leaves a trail referred to as data exhaust. It's just not feasible to keep moving very large amounts of raw data to centralized data stores – it is too big, changing too fast, and hyper distributed.

And it is ushering in what's referred to as **Analytics 3.0**, which is about connecting data generated at the edge with data that is stored in enterprise data centers. Consequently, some aspects of both storage and analytical capabilities have to be closer to the edge. Analytics 3.0 is essentially a combination of traditional business intelligence, big data and Internet of Things (IoT) distributed throughout the network.

The three eras of Analytics

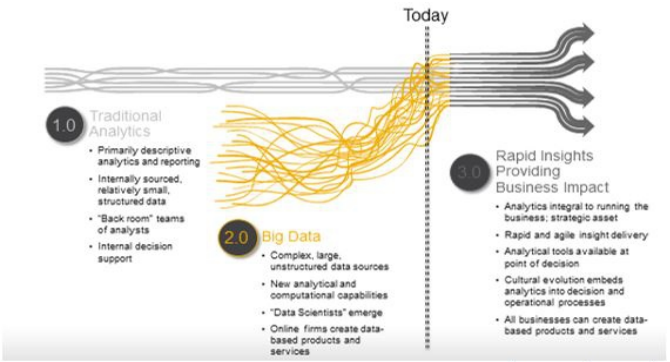


Image source: https://blogs.sap.com/wp-content/

What will be the next era of Analytics?

This question is little depressing as we have not even moved to Analytics 3.0 and the organisations have already working on the next era. The next era will be the "*Quantum Analytics*".

IBM, Google, Microsoft have built research labs and these companies and startups together have made some progress on the materials, designs and methods needed to make quantum computing possible. In theory, quantum computing takes advantage of subatomic and molecule interactions to perform operations on data to solve certain problems far faster than a binary conventional computer could.

संकाय स्तंभ (FACULTY COLUMN)

कंप्युटर सुरक्षा - खतरे और उपाय

यह एक कई अंको वाली सीरीज है। इस अंक में हम कम्प्युटर सुरक्षा से संबन्धित खतरे के बारे में चर्चा करेंगे। और आने वाले अंकों में कम्प्युटर सुरक्षा के उपायों और अन्य विषयों के बारे में चर्चा करेंगे।

आप जानते हैं कि कारें हर दिन चोरी हो जाती हैं, इसलिए आप शायद दरवाजे को बंद करने, गैरेज में पार्किंग करने या कार अलार्म का उपयोग करने जैसे उपाय करते हैं। उसी तरह, आपको अपने कंप्यूटर और डेटा के सामने आने वाले खतरों के बारे में पता होना चाहिए, और साथ ही उनकी सुरक्षा के लिए उपाय करना चाहिए। कुछ निवारक कदम उठाकर, आप न केवल अपने हार्डवेयर, सॉफ्टवेयर और डेटा की सुरक्षा कर सकते हैं, बल्कि खुद भी।

एक सार्थक कंप्यूटर सुरक्षा के लिए पहला कदम है जागरूकता। हमको उन सभी मामलों के बारे में जानना-समझना जरूरी है जो आपके कंप्युटर को खतरों में डालते हैं। आपको यह जानना होगा कि प्रत्येक खतरा आपको कैसे प्रभावित कर सकता है और दूर करने की क्या प्राथमिकता होगी। चलिए इससे संबंधित कुछ महत्वपूर्ण तत्वों के बारे में बात करते हैं-

खतरे (Threats)

कंप्यूटर सुरक्षा का पूरा उद्देश्य खतरों से बचाव या सुरक्षा करना है। एक खतरा कुछ भी हो सकता है जो नुकसान पहुंचा सकता है। कंप्यूटर सुरक्षा के संदर्भ में, एक खतरा चोर, वायरस, भूकंप या एक साधारण उपयोगकर्ता त्रुटि हो सकती है। वैसे एक खतरा तब तक नुकसानदायक नहीं हो सकता जब तक वह किसी उपलब्ध भेद्यता या कमजोरी का फायदा न उठाए।

भेद्यता (Vulnerability)

एक भेद्यता, एक कमजोरी है। यह एक ऐसी कोई भी चीज जो खतरों से सुरक्षित नहीं है, जिससे उसे नुकसान पहुँचता है। उदाहरण के लिए, एक अनलॉक कार की चोरी की संभावनाए होती हैं। भेद्यता व्यर्थ है जब तक किसी को इसकी जानकारी न हो। यदि आप शायद हमेशा अपनी कार को लॉक करते हैं या सुरक्षित स्थान पर पार्क करते हैं, तो चोर अगर पास में भी तो चोरी की संभावना नहीं होती है।

जोखिम

जोखिम से तात्पर्य उस हानि या क्षति की संभावना से है जब कोई खतरा भेद्यता का शोषण करता है। वैकल्पिक रूप से हम कह सकते हैं कि जोखिम = खतरा x भेद्यता। जोखिम के उदाहरणों में व्यावसायिक व्यवधान के परिणामस्वरूप वित्तीय नुकसान, गोपनीयता की हानि, प्रतिष्ठित क्षति, कानूनी निहितार्थ और यहां तक कि जीवन की हानि भी शामिल हो सकती है।

नुकसान की सीमा

कोई खतरा क्या? है और वो कितना नुकसान पहुचा सकता है? यह जानकर हम नुकसान की सीमा का आँकलन कर सकते हैं। जैसे, यदि आप एक पहाड़ की चोटी पर रहते हैं, तो बाढ़ का खतरा नहीं होगा। इसी तरह से, यदि आप एंटीवायरस सॉफ्टवेयर का उपयोग नहीं करते हैं, तो आपका कंप्यूटर संक्रमित हो जाएगा, खासकर तब जब वो इंटरनेट से जुड़ा हो। क्योंकि आप नुकसान की संभावना का अनुमान लगा सकते हैं जो विभिन्न खतरे पैदा कर सकते हैं और तदनुसार, आप उन्हें प्राथमिकता दे सकते हैं। आप यह तय कर सकते हैं कि कौन से खतरे अधिक हैं और उनके खिलाफ सावधानी बरत सकते हैं। जब लोग अपने कंप्यूटर सिस्टम को नुकसान पहुंचने के तरीकों के बारे में सोचते हैं, तो सामान्यतः वे केवल हार्डवेयर के नुकसान या डेटा के नुकसान के बारे में सोचते हैं। वास्तव में, कंप्यूटर सिस्टम को कई तरह से नुकसान हो सकता है। आपके महत्वपूर्ण डेटा के नुकसान से लेकर गोपनीयता के नुकसान तक, वास्तविक शारीरिक नुकसान तक, कई तरह के नुकसान उठा सकते हैं। अपने कंप्यूटर सिस्टम की सुरक्षा करते समय उन सभी संभावित प्रकारों के बारे में ध्यान देना जरूरी है जो आपके लिए नुकसानदायक हो सकते हैं। एक बुरा वायरस या हैकर आपके डेटा के साथ-साथ आपके प्रोग्राम को भी मिटा सकता है। यदि नेटवर्क से जुड़े हुए एक पीसी में समस्याए आती है तो इसकी संभावना ज्यादा है कि इससे जुड़े अन्य पीसीस् में समस्याए आए। साथ ही यदि कार्यालय या परिसर या बाढ़ से कोई नुकसान पहुँचता है तो वह रखे कंप्युटर सिस्टम्स और उनमें संग्रहीत डेटा को भी नुकसान हो सकता है।

सुरक्षा उपाय

किसी खतरे से बचने के लिए आप जो भी कदम उठाते हैं, जैसे अपने आप को, अपने डेटा या अपने कंप्यूटर को नुकसान से बचाने के लिए, वे आपके सुरक्षा उपाय कहलाये जाएंगे। उदाहरण के लिए, नियमित रूप से अपने डेटा का बैकअप लेना, डेटा हानि के खतरे के प्रति प्रतिकार (countermeasures) या सुरक्षा है। एक फायरवॉल हैकर्स के खिलाफ प्रतिवाद है। प्रतिवाद के दो वर्ग हैं। पहले उपयोगकर्ता को व्यक्तिगत नुकसान से बचाता है, जैसे कि व्यक्तिगत संपत्ति, गोपनीय जानकारी, वित्तीय रिकॉर्ड, चिकित्सा रिकॉर्ड, आदि। दूसरा प्रतिकार कंप्युटर सिस्टम्स, कंप्यूटर में सग्रहित और संसाधित डेटा को चोरी, नष्ट होने, बिजली की समस्याओं, प्राकृतिक आपदाओं या हमलों से बचाता है।

उपयोगकर्ताओं (Users) के लिए खतरा

इंटरनेट, जो लगभग सभी के लिए उपलब्ध है, वस्तुतः किसी भी तरह के उपयोग के लिए भी यह कई खतरों के लिए एक स्त्रोत है। फिर भी, हम कंप्यूटर से संबंधित सभी समस्याओं के लिए इंटरनेट को दोष नहीं दे सकते। जैसे कि पहचान की चोरी, अभी भी कंप्यूटर की बिना मदद या बहुत कम मदद से पूरा किया जाता है। अन्य, जैसे कि कंप्यूटर के उपयोग से होने वाली चोंटों में अक्सर खराब डिजाइन या खराब काम की आदतों का दोष होता है।

पहचान की चोरी

यह चोरी तब होती है जब कोई व्यक्ति आपके नाम, आधार नंबर, पैन नंबर या अन्य व्यक्तिगत जानकारी का उपयोग करके आपके नाम से दस्तावेज या क्रेडिट प्राप्त करता है। सही जानकारी के साथ, एक पहचान चोर वस्तुतः पीड़ित बन सकता है और पीड़ित के नाम पर ड्राइवर लाइसेंस, बैंक खाते, बंधक, और अन्य सामान प्राप्त कर सकता है। आइडेंटिटी (पहचान) चोर अपनी जरूरत की जानकारी हासिल करने के लिए कम तकनीक के साथ-साथ उच्च तकनीक का इस्तेमाल कर सकते हैं।

आईए अब हम कुछ तकनीकों के बारे में समझते हैं -

शोल्डर सर्फिंग

किसी को देखते समय यह एक साधारण ट्रिक है जिसमें पहचान चोर आपके पास खड़ा होकर वह आपको अपनी व्यक्तिगत जानकारी, पासवर्ड या एटीएम में पिन आदि दर्ज करते हुए देख रहा हो।

स्नैगिंग

एक चोर टेलीफोन, एक्सटेंशन लाइन, वायरटैप या क्यूबिकल वॉल पर सुनकर स्नैगिंग की कोशिश कर सकता है जबकि पीड़ित एक वैध एजेंट को क्रेडिट कार्ड या अन्य व्यक्तिगत जानकारी देता है। जिसे ईव्सड्रॉपिंग भी कहा जाता है।

डंपस्टर डाइविंग

यह एक बहुत ही कम तकनीकी दृष्टिकोण वाली विधि है। रद्द किए गए चेक, क्रेडिट कार्ड स्टेटमेंट या बैंक खाते, जिसे किसी ने लापरवाही से कूड़े के डिब्बे में फेंक दिया हो, को पहचान चोर कूड़े के डिब्बे से खंगालकर व्यक्तिगत जानकारी निकलते हैं।

सोशल इंजीनियरिंग

एक चोर आपको दोस्त बना सकता है, आपके करीब आता है और धीरे-धीरे विश्वास के बाद वह आपकी निजी जानकारी चुरा लेता है। या वह दिखावा करता है कि वह अधिकृत बैंक या किसी एजेंसी से है और आपसे आपकी वित्तीय जानकारी या एटीएम आदि में पिन मांगता है। वर्तमान में यह एक उपयोगी तरीका है। वित्तीय धोखा देने में अधिकांशतः इसका उपयोग किया जाता है।

संकाय स्तंभ (FACULTY COLUMN)

कंप्युटर सुरक्षा- खतरे और उपाय

हाई-टेक तरीके

परिष्कृत आईडी चोर, कंप्यूटर और इंटरनेट कनेक्शन का उपयोग करके जानकारी प्राप्त कर सकते हैं। उदाहरण के लिए, ट्रोजन हॉर्स को सिस्टम पर लगाया जा सकता है या असुरक्षित इंटरनेट साइटों से किसी व्यक्ति की पहचान छीनी जा सकती है। क्रेडिट कार्ड और वित्तीय लेनदेन की अखंडता और गोपनीयता सुनिश्चित करने के लिए सिक्योर सॉकेट्स लेयर (एसएसएल) और सिक्योर एचटीटीपी (एस-एचटीटीपी) जैसी सुरक्षा तकनीकों के सामान्य उपयोग के कारण यह सामान्यतः प्रयोग में नहीं आती है। संचारित डेटा की सुरक्षा पर इतना ध्यान दिया जाता है कि, सोशल इंजीनियरिंग और कम तकनीक वाली विधियाँ ही पहचान की चोरी के प्रमुख स्रोत हैं।

गोपनीयता की हानि

कई कंपनियां जो स्थानीय सुपरमार्केट से लेकर अपनी बीमा कंपनी तक हो सकती है, आपके बारे में जानकारी इकट्ठा करती है जब आप उनकी सेवाओं और वस्तुओं का उपयोग करते हैं और यह जानकारी अपने डेटाबेस में बनाए रखती है। आप इन फर्मों से आपका नाम और पता जानने की उम्मीद कर सकते हैं, लेकिन आपको यह जानकर हैरानी होगी कि वे जानते हैं कि हर महीने आप अपनी कार में कितनी बार गैस डालते हैं या एक पत्रिका खरीदते हैं। और बहुत सी कंपनियां इस जानकारी को गोपनीय नहीं रखती हैं; वे इसे अन्य कंपनियों को बेच सकते हैं जो आपके बारे में जानने में रुचि रखते हैं।

ऑनलाइन जासूसी माध्यम

सॉफ्टवेयर डेवलपर्स ने आपकी गतिविधियों को ऑनलाइन ट्रैक करने के कई तरीके बनाए हैं। हालाँकि इन तरीकों में से कई सौम्य उद्देश्यों के लिए बनाए गए थे - जैसे वैध वेबमास्टर्स को यह निर्धारित करने में मदद करते हैं कि कौन उनकी साइटों पर सबसे अधिक बार आता है। इनका उपयोग उन तरीकों से भी किया जा रहा है जो अधिकांश उपभोक्ता सराहना नहीं करते हैं।

कूकीज

एक कुकी एक छोटी पाठ (text) फ़ाइल है जो एक वेब सर्वर आपके ब्राउज़र को आपके कंप्यूटर पर रखने के लिए कहता है। कुकी में वह जानकारी होती है जो आपके कंप्यूटर (उसके आईपी पते), आपकी (आपके उपयोगकर्ता नाम या ई-मेल पते), और आपकी वेब साइट पर जाने की जानकारी की पहचान करती है। उदाहरण के लिए, कुकी अंतिम बार आपके द्वारा साइट पर जाने, आपके द्वारा डाउनलोड किए गए पृष्ठों को देखने और जाने से पहले साइट पर कितनी देर तक आप थे, हो सकती है। यदि आप एक वेब साइट जैसे ई-कॉमर्स साइट पर एक खाता स्थापित करते हैं, तो कुकी में आपके खाते के बारे में जानकारी होगी, जिससे जब भी आप उस साइट पर जाते हैं, तो सर्वर को ढूंढना और प्रबंधित करना आसान हो जाता है। उपयोगी उद्देश्य के बावजूद, कुकीज को अब गोपनीयता के लिए एक महत्वपूर्ण खतरा माना जाता है। ऐसा इसलिए है क्योंकि उनका उपयोग कई प्रकार की सूचनाओं को संग्रहीत और रिपोर्ट करने के लिए किया जा सकता है। उदाहरण के लिए, एक कुकी उन सभी साइट सूची स्टोर करके रख सकती है जिन पर आप गए थे। यह डेटा उस साइट पर स्थानांतरित किया जा सकता है जिसने कुकी को आपके सिस्टम पर रखा है, और उस जानकारी का उपयोग आपकी इच्छा के विरुद्ध किया जा सकता है। उदाहरण के लिए, अगली बार जब आप वेब साइट पर जाते हैं, तो स्क्रीन पर दिखाई देने वाले विज्ञापन के निर्धारण हेतु, कुकी के निर्माता कुकी का उपयोग कर सकते हैं। कई वेबमास्टर अपनी साइट के दर्शकों के जनसांख्यिकीय मैप को निर्धारित करने के लिए कुकीज से जानकारी का उपयोग करते हैं। इससे भी बदतर, कुकीज को आधार के रूप में इस्तेमाल करते हुए हैकर के हमलों को क्रियान्वित किया जा सकता है।

वेब बग्स

एक वेब बग एक छोटी सी GIF- प्रारूप छवि फ़ाइल है जिसे वेब पेज या HTML- प्रारूप ई-मेल संदेश में एम्बेड किया जा सकता है। एक वेब बग आकार में एक एकल पिक्सेल जितना छोटा हो सकता है और HTML दस्तावेज में कहीं भी आसानी से छिपाया जा सकता है। हालांकि, छोटी छवि के पीछे एक कोड होता है जो एक कुकी के रूप में एक ही तरह से कार्य करता है, आपकी कई ऑनलाइन गतिविधियों को ट्रैक करने की बग के निर्माता को अनुमति देता है। एक बग, आपके द्वारा देखे गए वेब पृष्ठों, सर्च इंजन में टाइप किए गए कीवर्ड, वेब फर्म में इंटर कि गई व्यक्तिगत जानकारी एवं अन्य स्त्रोतों में छुपे होते हैं। काइयों द्वारा यह माना जाता है कि यह एक जासूसी उपकरण (eavesdropping device) हैं। वेब बग्स के बारे में जानने के बाद, अधिकांश उपभोक्ता उन्हें हराने का तरीका खोजते हैं। अब कई वेब-बग विरोधी प्रोग्राम मौजूद हैं।

स्पाइवेयर

स्पाइवेयर शब्द का इस्तेमाल कई अलग-अलग प्रकार के सॉफ्टवेयर को संदर्भित करने के लिए किया जाता है जो कंप्यूटर उपयोगकर्ता की गतिविधियों को ट्रैक कर सकते हैं और उन्हें किसी और को रिपोर्ट कर सकते हैं। अब स्पायवेयर कार्यक्रमों की अनगिनत किस्में हैं। स्पाइवेयर के लिए एक और सामान्य शब्द एडवेयर है, क्योंकि इंटरनेट विज्ञापन स्पाइवेयर का एक सामान्य स्रोत है। कुछ प्रकार के स्पाइवेयर खुलेआम काम करते हैं। उदाहरण के लिए, जब आप किसी प्रोग्राम को इंस्टॉल और रजिस्टर करते हैं, तो यह आपको एक फॉर्म भरने के लिए कह सकता है। प्रोग्राम तब डेवलपर को जानकारी भेजता है जो इसे डेटाबेस में संग्रहीत करता है। जब इस तरीके से उपयोग किया जाता है तो स्पाइवेयर-प्रकार के कार्यक्रमों को पूरी तरह से वैध के रूप में देखा जाता है क्योंकि उपयोगकर्ता को पता है कि जानकारी एकत्र की जा रही है। आमतौर पर स्पाइवेयर को उपयोगकर्ता के ज्ञान के बिना कंप्यूटर पर स्थापित किया जाता है और वह उपयोगकर्ता की सहमति के बिना जानकारी एकत्र करता है। स्पाइवेयर आपके पीसी पर कई स्रोतों से आ सकता है जैसे वेब पेज, ई-मेल संदेश और पॉपअप विज्ञापन या अन्य कोई स्त्रोत। एक बार आपकी मशीन पर स्पाइवेयर स्थापित हो गया तो, वह वस्तुतः कुछ भी ट्रैक कर सकता है। स्पाइवेयर व्यक्तिगत कीस्ट्रोक्स, वेब उपयोग, ई-मेल पते, व्यक्तिगत जानकारी और अन्य प्रकार के डेटा रिकॉर्ड कर सकते हैं। आम तौर पर, प्रोग्राम एकत्रित डेटा को ई-मेल या एक वेब पेज के माध्यम से प्रसारित करता है।

स्पैम

हालांकि आपकी निजी जानकारी की उपलब्धता परेशान करने वाली हो सकती है, लेकिन अधिकांश उपयोगकर्ताओं के लिए इसका परिणाम स्पैम कहलाता है। स्पैम इंटरनेट "जंक मेल" है। आखिरकार, आपके ई-मेल पते को अक्सर उन व्यक्तिगत जानकारी में शामिल किया जाता है जो कंपनियां एकत्र करती हैं और साझा करती हैं। स्पैम के लिए सही शब्द अवांछित ई-मेल (UCE) है। लगभग सभी स्पैम वाणिज्यिक विज्ञापन हैं। आप सोच सकते हैं कि स्पैम ई-मेल का जवाब सरल है- बस संदेशों को आने पर हटा दें। लेकिन कई कंप्यूटर उपयोगकर्ताओं के लिए, स्पैम इस तरह के एक सरल समाधान के लिए बहुत बड़ी समस्या है। कुछ लोगों को दर्जनों, सैकड़ों, स्पैम संदेश प्रतिदिन मिलते हैं। समस्या व्यवसायों के लिए बहुत बड़ी है, जहां कॉर्पोरेट ई-मेल सर्वर अनावश्यक रूप से हर महीने अनगिनत स्पैम संदेशों को संग्रहीत और स्थानांतरित करते हैं। व्यक्तिगत स्तर पर, स्पैम प्राप्तकर्ताओं का समय अवांछित संदेशों की समीक्षा करने में बीतता है क्योंकि उन्हें डर होता है कि वे गलती से वैध मेल हटा सकते हैं। इस अकेले समय की बर्बादी में कई घंटे लगते हैं। इसलिए स्पैम का वास्तविक समाधान इसे उन सभी लोगों तक पहुंचने से पहले नियंत्रित करना है जो इसे नहीं चाहते हैं। इसे नियंत्रित करने के लिए स्पैम को परिभाषित करना महत्वपूर्ण है। एक व्यक्ति का महत्वपूर्ण संदेश दूसरे व्यक्ति का स्पैम हो सकता है। यह अंतर स्पैम रोकथाम के लिए कानूनी आधार निर्धारित करना कठिन बनाता है। २००३ के बाद से, स्पैम की विशेषताओं की कानूनी रूप से स्वीकृत परिभाषा वाणिज्यिक ई-मेल है जो एक समय में लाखों लोगों को संचारित किया जाता है। मात्रा और तथ्य यह है कि प्रत्येक संदेश में काफी समान सामग्री होती है जो स्पैम को परिभाषित करते हैं।

संकाय स्तंभ (FACULTY COLUMN)

कंप्युटर सुरक्षा- खतरे और उपाय

कंप्यूटर-संबंधित चोट

कंप्यूटर का उपयोग उपयोगकर्ता को शारीरिक चोट पहुंचा सकता है। लंबे समय तक मॉनीटर का उपयोग करना और बैठने की खराब स्थिति ऐसी चोटों के प्राथमिक कारण हैं।

हार्डवेयर के लिए खतरा

आपके कंप्यूटर के हार्डवेयर के खतरों में ऐसी घटनाएं शामिल हैं जिनका कंप्यूटर के संचालन या रखरखाव पर प्रभाव पड़ता है। वे इस तरह की नियमित चीजों से लेकर सिस्टम ब्रेकडाउन, उपकरणों की चोरी, विध्वंस, हार्डवेयर दुरुपयोग, सहित व्यक्तियों के दुर्भावनापूर्ण कार्यों का दुरुपयोग करते हैं। आग और बाढ़ जैसी आपदाएँ भी कंप्यूटर के हार्डवेयर के लिए खतरे हैं।

बिजली से संबंधित खतरे

बिजली की समस्याएं कंप्यूटर को दो तरह से प्रभावित करती हैं। बिजली उतार-चढ़ाव-जब आपकी विद्युत सेवा की ताकत बढ़ती है या गिरती है, घटक विफलता (कम्पोनन्ट फैल्यर) का कारण बन सकती है। बिजली की विफलता-जब बिजली पूरी तरह से खो (लोस्ट) जाती है, तो सिस्टम बंद हो जाता है। बिजली की विफलता और उतार-चढ़ाव दोनों के परिणामस्वरूप डेटा का नुकसान हो सकता है।

चोरी और बर्बरता

एक चोर या बर्बरता एक कंप्यूटर को जबरदस्त नुकसान पहुंचा सकती है, जिसके परिणामस्वरूप सिस्टम का और उसमें स्टोर्ड डेटा का पूरा नुकसान हो सकता है। यह भी एक तथ्य है कि बहुत कम मकान-मालिक और छात्र अपने पीसी को जानबूझकर विनाशकारी कृत्यों से बचाने के लिए सावधानी बरतते हैं। चोरों और बदमाशों को अपने सिस्टम्स से दूर रखने का सबसे अच्छा तरीका है कि आप अपने सिस्टम को सुरक्षित क्षेत्र में रखें। विशेष तरह के ताले उपलब्ध हैं जो कि एक डेस्क पर सिस्टम यूनिट, मॉनिटर या अन्य उपकरण अच्छी तरह से बांधकर रख कर सकते हैं, जिससे सिस्टम्स को स्थानांतरित करना बहुत मुश्किल है। होम अलार्म सिस्टम एक अच्छा निवेश है जब आपके महंगे उपकरण और अनमोल डेटा दांव पर हो।

प्राकृतिक आपदाएँ

आपदा नियोजन प्राकृतिक और मानव निर्मित आपदाओं को संबोधित करता है। इसे "आपदा रोकथाम" नहीं कहा जाता है क्योंकि भूकंप और तूफान जैसी चीजें भविष्यवाणी करना मुश्किल है और रोकथाम करना असंभव है। हालाँकि, आप उनके लिए योजना बना सकते हैं। एक अच्छी तरह से सोची-समझी योजना डेटा/इनफार्मेशन के नुकसान और काम में रुकावट को कम कर सकती है। क्योंकि प्राकृतिक आपदाएँ स्थान के अनुसार बदलती हैं, इसलिए आपका पहला कदम उन सभी आपदाओं की एक सूची बनाना है जो आपको लगता है कि आपके क्षेत्र में हो सकती है और फिर उस सूची को प्राथमिकता तय करना है उदाहरण के लिए, कोई फर्क नहीं पड़ता कि आप कहाँ रहते हैं, घर में आग लगने की संभावना बवंडर से ज्यादा होती है। भले ही बवंडर अधिक विनाशकारी हो, आपके पास बारम्बार होने वाली आपदाओं से निपटने के लिए योजनाएं होनी चाहिए। इससे कोई फर्क नहीं पड़ता कि आप अपनी सूची होने वाली कौन-कौन से आपदाएँ शामिल हैं, आपके प्रतिवादों (काउन्टरमेजर्स) में जागरूकता, पूर्वानुमान और तैयारी शामिल होनी चाहिए। पहले दो प्रतिवाद सरल हैं: ध्यान रखें कि आपदा कभी भी आ सकती है और अनुकूल समय में आपदा के आने का पूर्वानुमान लगाया जा सकता है। उदाहरण के लिए, यदि आप भारत के पूर्वी तट पर रहते हैं, तो आप जानते हैं कि तूफान का पूर्वानुमान कब लगाया जाए।

डेटा को खतरा

कंप्यूटर का उद्देश्य किसी तरह से जानकारी बनाने के लिए डेटा को संसाधित (प्रोसेस) करना है। कंप्यूटर सुरक्षा का लक्ष्य इस प्रक्रिया को आगे बढ़ाना है। क्योंकि डेटा और जानकारी अमूर्त(इंटेनजीबल) हैं, इसलिए यह मिशन कठिन है। इसके बावजूद, आपको पहचानने वाले हर खतरे से मूल्य की हर चीज को बचाने का प्रयास करना चाहिए। खतरे की तीन सामान्य श्रेणियां हैं: दुर्भावनापूर्ण कोड और मैलवेयर, आपराधिक कृत्य और साइबर आतंकवाद।

मैलवेयर, वायरस और दुर्भावनापूर्ण प्रोग्राम

मैलवेयर शब्द वायरसेस, वॉर्म्स, ट्रोजन हॉर्स अटैक एप्लेट और अटैक स्क्रिप्ट का वर्णन करता है। ये वायरल प्रोग्राम आपकी डेटा के लिए आम खतरे का प्रतिनिधित्व करते हैं। वायरस एक छोटा कंप्यूटर प्रोग्राम (कोड) है जो खुद को होस्ट प्रोग्राम से जोड़ता है। वॉर्म्स नेटवर्क सिस्टम्स के लिए विशेष रूप से होते हैं, किसी भी नेटवर्क पर अन्य मशीनों तक फैलते हैं जो आपके कंप्यूटर से जुड़े होते हैं और कंप्यूटर पर पूर्वनिर्धारित (प्रीप्रोग्राम) किए गए हमले करते हैं। ट्रोजन हॉर्स, उनके नाम की तरह, एक उपयोगी प्रोग्राम की आड़ में दुर्भावनापूर्ण कोड को सिस्टम में स्थापित करते हैं। मैलवेयर का एक अन्य रूप एक हमले की स्क्रिप्ट है जो विशेष रूप से विशेषज्ञ प्रोग्रामर द्वारा इंटरनेट का शोषण करने के लिए लिखा जाता है। एक और खतरा, वेब पेजों में छिपे जावा एप्लेट का है। इन्हें तब लॉन्च किया जाता है जब उपयोगकर्ता के ब्राउजर से उन वेब पेजों पर जाया जाता है।

साइबर अपराध

कंप्यूटर अपराध (साइबर क्राइम) का उद्देश्य कंप्यूटर चोरी करना, सूचनाओं को नुकसान पहुंचाना या सूचनाओं की चोरी करना है। कंप्यूटर अपराध का मूल रूप से तकनीकी होना आवश्यक नहीं है। कंप्यूटर के खिलाफ अधिकांश आपराधिक कृत्यों में सीधे प्रौद्योगिकी शामिल नहीं है। किसी भी पारंपरिक आपराधिक कृत्य, जैसे धोखाधड़ी, को अंजाम देने के लिए कंप्यूटर का उपयोग साइबर क्राइम कहलाता है और यह एक बढ़ता हुआ खतरा है। साइबर अपराध इतनी तेजी से बढ़ रहा है कि संघीय और राज्य सरकारों ने कंप्यूटर से संबंधित अपराधों से निपटने के लिए बहुत सी एजेंसियां बनाई हैं। जैसे सर्ट-इन।

हैकिंग

हैकिंग साइबर अपराध का सबसे आम रूप है, और यह लगातार लोकप्रिय हो रहा है। एक हैकर वह है जो एक कंप्यूटर और नेटवर्क या इंटरनेट कनेक्शन का उपयोग किसी अन्य कंप्यूटर या सिस्टम में घुसपैठ कर गैरकानूनी कार्य को अंजाम देता है। यह सरल अतिचार (ट्रेस्पास) या कृत्य है जो डेटा को दूषित, नष्ट, या बदलने का कार्य कर सकता है। एक अन्य रूप में, हैकिंग एक वितरित इंकार सेवा (डिस्ट्रीबूटेड डिनाइअल ऑफ सर्विस-डीडीओएस) हमले का आधार हो सकता है, जिसमें एक हैकर कई गैर संदिग्ध पीड़ितों के पीसी पर दुर्भावनापूर्ण कोड छिपाता है। यह कोड हैकर को संक्रमित पीसी पर ले जाने में सक्षम कर सकता है, या बस उन्हें वेब सर्वर को अनुरोध भेजने के लिए उपयोग कर सकता है। यदि हैकर पर्याप्त पीसी को नियंत्रित करता है, और उन्हें लक्षित वेब सर्वर को पर्याप्त अनुरोध भेजने के लिए उपयोग कर सकता है, तो सर्वर बहुर सारे अनुरोधों के साथ जाम हो जाता है और काम करना बंद कर देता है। सफल डीडीओएस हमलों से शिकार कंपनियों को इससे खुद की सुरक्षा में लाखों खर्च करना पड़ सकता है।

एक समय में, एक हैकर सिर्फ एक व्यक्ति था जो कंप्यूटर को अच्छी तरह से समझता था; हालांकि, हैकिंग अब आपराधिक या विरोधी सामाजिक गतिविधि को संदर्भित करता है। आज, हैकर की गतिविधियों को आमतौर पर उनके इरादे से वर्गीकृत किया जाता है। जैसे मनोरंजन के लिए हमले, व्यवसायीक या वित्तीय हमले, खुफिया हमले, गंभीर व सैन्य हमले और आतंकवादी हमलों। गोपनीयता पर आक्रमण के अलावा, मनोरंजक हैकिंग अपेक्षाकृत हानिरहित है। ज्यादातर मामलों में, मनोरंजक हैकर बिना किसी नुकसान के अपनी क्षमताओं को साबित करने का प्रयास करते हैं। व्यापार, वित्तीय या खुफिया हमलों में, हालांकि, हैकर्स अक्सर डेटा डीडलिंग में संलग्न होते हैं। जैसे व्यक्तिगत लाभ के लिए रिकॉर्ड बनाने या बदलने में या लक्षित सिस्टम से डेटा को कॉपी करने के प्रयत्न में। किसी व्यक्ति या संगठन के खिलाफ शिकायत/बैर होने पर हैकर्स द्वारा गंभीर हमले किए जाते हैं और ऐसे हमले अक्सर विनाशकारी होते हैं। आतंकवादी हमलों से विनाशकारी नुकसान हो सकता है। औद्योगिक दुनिया अपने कंप्यूटरों पर अत्यधिक निर्भर है और इस बात का सबूत है कि इस प्रकार का हमला भविष्य के युद्ध का एक माध्यम हो सकता है।

संकाय स्तंभ (FACULTY COLUMN)

कंप्युटर सुरक्षा- खतरे और उपाय

कॉमन हैकिंग मेथड्स

हैकर्स कंप्यूटर सिस्टम में सेंध लगाने के लिए कई तरह के तरीकों का इस्तेमाल करते हैं। ये विधियाँ तीन व्यापक श्रेणियों में आती हैं।

स्नीफींग

स्नीफींग का प्रयोग किसी उपयोगकर्ता के पासवर्ड को जानने के लिए किया जाता है। पासवर्ड का पता करने के तीन तरीके हैं-पासवर्ड साझा करना, पासवर्ड का अनुमान लगाना, और पासवर्ड कैप्चर करना। पासवर्ड साझा करना सबसे आम है और तब होता है जब कोई पीड़ित व्यक्ति किसी हैकर को अपना पासवर्ड बताता है। पासवर्ड को साधारण अज्ञानता के कारण साझा किया जाता है और पीड़ितों को यह पता नहीं चलता है कि पासवर्ड का उपयोग उनकी इच्छा के विरुद्ध या उन तरीकों से किया जा सकता है, जो वे कभी नहीं करेंगे। पासवर्ड का अनुमान लगाना ठीक वैसे ही होता है जैसे शब्द का अर्थ होता है: एक हैकर उपयोगकर्ता के पासवर्ड का अनुमान लगाने की कोशिश करता है और तब तक कोशिश करता रहता है जब तक कि वह सही नहीं हो जाता। उपयोगकर्ता जटिल पासवर्ड का उपयोग करके पासवर्ड अनुमान लगाने से सुरक्षित रह सकते हैं। नेटवर्क व्यवस्थापक नेटवर्क में लॉग इन करने के लिए किसी के भी प्रयासों की संख्या को सीमित करके अनुमान लगाने से रोक सकते हैं। पासवर्ड कैप्चर में, पासवर्ड किसी प्रकार के मैलवेयर प्रोग्राम द्वारा प्राप्त किया जाता है और हैकर को भेज दिया जाता है। पासवर्ड इलेक्ट्रॉनिक रूप से कैप्चर किए जा सकते हैं और उन्हें टेक्स्ट के रूप में भेजा जाता है जो एन्क्रिप्टेड नहीं है। उदाहरण के लिए, एक लॉगिन सत्र के दौरान, एक हैकर पासवर्ड डेटा को तब इंटरसेप्ट कर सकता है जब इसे सर्वर पर भेजा जाता है, भले ही यह सिस्टम के भीतर ही एन्क्रिप्ट किया गया हो।

सोशल इंजीनियरिंग

सोशल इंजीनियरिंग को "विश्वसनीय खेल चलाना" कहा जाता था। हैकर किसी भी तरह के धोखाधड़ी का इस्तेमाल कर पासवर्ड को पीड़ितों से प्राप्त कर सकता है। यह डंपस्टर डाइविंग जितना ही सरल हो सकता है। पहचान की चोरी के लिए एक पासवर्ड चोर उपयोगी पहुँच जानकारी खोजने के लिए पीड़ित के कूड़े को खँगालता है। सोशल इंजीनियरिंग का एक अन्य रूप "फोन सर्वेक्षण", "एप्लिकेशन", और "आपातकालीन स्थिति" है। इन स्थितियों में, एक हैकर फोन या ई-मेल से संभावित पीड़ितों से संपर्क कर सकता है और पीड़ितों से एक वैध प्रतीत होते कारण के लिए पासवर्ड की जानकारी प्राप्त करने की कोशिश कर सकता है। इस पद्धति को कभी-कभी फिशिंग भी कहा जाता है।

स्पूफिंग

हैकर्स ई-मेल हेडर को बदल सकते हैं ताकि यह प्रतीत हो सके कि जानकारी के लिए एक अनुरोध दूसरे पते से उत्पन्न हुआ है। इसे स्पूफिंग कहा जाता है। वे वैध कंप्यूटर पर होने का नाटक करके इलेक्ट्रॉनिक प्रविष्टि प्राप्त कर सकते हैं; जिसे आईपी-स्पूफिंग कहा जाता है। इस तकनीक का उपयोग करते हुए, हैकर एक संदेश को इंटरसेप्ट करता है या एक अधिकृत उपयोगकर्ता के रूप में प्रतीत होते हुये सिस्टम तक पहुंच प्राप्त करता है। नेटवर्क में, यह संदेश जानकारी को बदलकर यह प्रकट करने के लिए किया जाता है कि यह एक विश्वसनीय कंप्यूटर से उत्पन्न हुआ है।

साइबरटर्मिज्म

साइबरवेयर और साइबरबैटरिज्म (सायबर आतंकवाद) युद्ध के नए रूप में राष्ट्र के महत्वपूर्ण सूचना बुनियादी ढांचे पर हमला करते हैं। साइबर आतंकवाद के मामले में पारंपरिक लक्ष्य प्रमुख कंप्यूटर सिस्टम, या डिजिटल नियंत्रण को नुकसान पहुंचाना या नियंत्रित करना है। यह एक अप्रत्यक्ष उद्देश्य को पूरा करने के लिए किया जाता है जैसे कि पावर ग्रिड या दूरसंचार को बाधित करना। सायबर आतंकवाद के लिए विशिष्ट लक्ष्य बिजली संयंत्र, परमाणु सुविधाएं, जल उपचार संयंत्र और सरकारी एजेंसियां हैं। हालांकि, नेटवर्क-आधारित निगरानी और नियंत्रण प्रणाली वाली कोई भी साइट इंटरनेट से सायबर आतंकवाद के लिए लक्ष्य हो सकती है।

(साभारः पीटर नॉर्टन द्वारा लिखित इंट्रोडक्शन टु कंप्यूटर्स)

Suspense Account

Reserve Bank of India is the main banker of the Government and other authorised Banks function as its agents while handling Government transactions. Transactions through Banks have their final impact on Government 'Cash Balance' in course of time. Prior to that certain intermediary/ adjusting heads are operated. Some of these intermediary heads (known as **Suspense Heads**) are-

- 8670 Cheques and Bills
- 8658 Suspense Accounts -108 PSB Suspense
- 8675 Deposits with Reserve Bank - 101 Central-Civil

While in Government Accounts Items of receipts and payments which cannot at once be taken to a final head of receipt or expenditure owing to lack of information as to the nature or for any other reasons are to be booked temporarily under the Major Head **8658—Suspense Accounts** under L-suspense and Miscellaneous of the List of Major and Minor Heads of Account. The Suspense Heads are to be cleared by (—) Debit or (—) Credit as the case may be on receipt of' the relevant details/information.

Definition for Suspense Account-

- A **suspense account** is an account in the books of an organization in which items are entered temporarily before allocation to the correct or final account.
- A **suspense account** is an account used temporarily or permanently to carry doubtful entries and discrepancies pending their analysis and permanent classification.

As the definition suggest suspense account is an intermediary account used in-between two or more transaction where direct settlement is not possible, thus it have vast use in Government accounting. Suspense account is a non-interest bearing account. All transactions involving suspense account are reported to RBI.

Various minor heads below major head **8658-Suspense Accounts** viz Pay and Accounts Office Suspense, Suspense Account (Civil), Tele-Communication Accounts Office Suspense, Tax Deducted at Source Suspense, etc. Under these minor heads, there are several sub heads to accommodate different nature of transactions under these minor/sub heads, various accounting authorities constitute separate detailed heads.

e.g. In case of offices following the Public Works/Forest Divisional system of accounts, the amount of paid cheques will be adjusted as under:

(-) Cr. 8782-Cash Remittances

102 Public Works Remittances or 103 Forest Remittances (as the case may be)

Cr. 8658—Suspense Accounts 108 Public Sector Bank Suspense

Public Private Partnership: Definition and Characteristics

PPP is public–private co-operation model having its own legal provisions, contractual relations, clear implementation strategies and prior agreement about sharing of risks and benefits. The notion of development strategy of PPP is widely accepted by most of the researchers. Since the PPP maximizes benefits for development through collaboration and enhanced efficiency, this has emerged as a new development arrangement. The PPP Knowledge Lab of World Bank Group defines PPP as "*a long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance*".

The Department of Economic Affairs, Government of India defines PPPs as:

PPP means an arrangement between a government or statutory entity or government owned entity on one side and a private sector entity on the other, for the provision of public assets and/ or related services for public benefit, through investments being made by and/or management undertaken the private sector entity for a specified time period, where there is a substantial risk sharing with the private sector and the private sector receives performance linked payments that conform (or are benchmarked) to specified, pre-determined and measurable performance standards.

However, the definition given under the scheme and guidelines for the India Infrastructure Project Development Fund is little more specific. It states PPP as, Partnership between a public sector entity (Sponsoring authority) and a private sector entity (a legal entity in which 51% or more of equity is with the private partner/s) for the creation and/or management of infrastructure for public purpose for a specified period of time (concession period) on commercial terms and in which the private partner has been selected through a transparent and open procurement system.

CHARACTERISTICS OF PPP

A government of India, through the Ministry of Finance has developed a toolkit as a part of a PPP capacity building programme with funding support from the World Bank, AusAID South Asia Region Infrastructure for Growth Initiative and the Public Private Infrastructure Advisory Facility (PPIAF). A consulting consortium, consisting of ECA and CRIS, commissioned by the World Bank, has prepared this Toolkit based on extensive external consultations.

The said toolkit has given the characteristics of PPP as follows:

(1) The private sector is responsible for carrying out or operating the project and takes on a substantial portion of the associated project risks.

(2) During the operational life of the project the public sector's role is to monitor the performance of the private partner and enforce the terms of the contract.

(3) The cost of the private sector may be recovered in whole or in part from charges related to the use of the services provided by the project, and may be recovered through payments from the public sector.

(4) The payments of public sector are based on performance standards set out in the contract.

(5) More often the private sector will contribute the majority of the project's capital costs.

Overview of the OIOS

Introduction

The 'One IA&AD One System' OIOS project aims at creating a single source of truth regarding audit activities of IA&AD. As we all are aware that IA&AD has several other IT applications like e-office, IAAD KMS, and so many others to cater to the needs of one or more offices.
OIOS is Web based application. Web based application is based around the idea of a Client and at least one Server computer connected via a network such as the World Wide Web. The client is the machine the customer sits in front. He/She interrogates with a server machine with the aid of a 'browser', a package able to display Hypertext markup language (HTML) content which is both graphical, textual and occasionally multi-media (sound and pictures) can be produced easily from within a package.

Objective

- OIOS aims at creating a single source of truth regarding the audit activities.
- Activity and process must be captured in OIOS, basically to avoid post facto data entry to the maximum extent.
- To make the process more streamlined.
- Shifting from traditional way to digital Mode.

Module

As many web based applications have their modules based on user requirement. This web based application has various modules configured and used by any audit office in the IA&AD. OIOS is broadly divided into 16 modules. These modules provides flexibility to onboard specific field audit offices or parts of field audit offices or specific activities across offices.
Each of these modules produces output which can be downloaded and printed like audit products, audit enquiries, audit observation and so on.
Following is the list of business module along with their objectives in OIOS as detailed in the table below.

संकाय स्तंभ (FACULTY COLUMN)

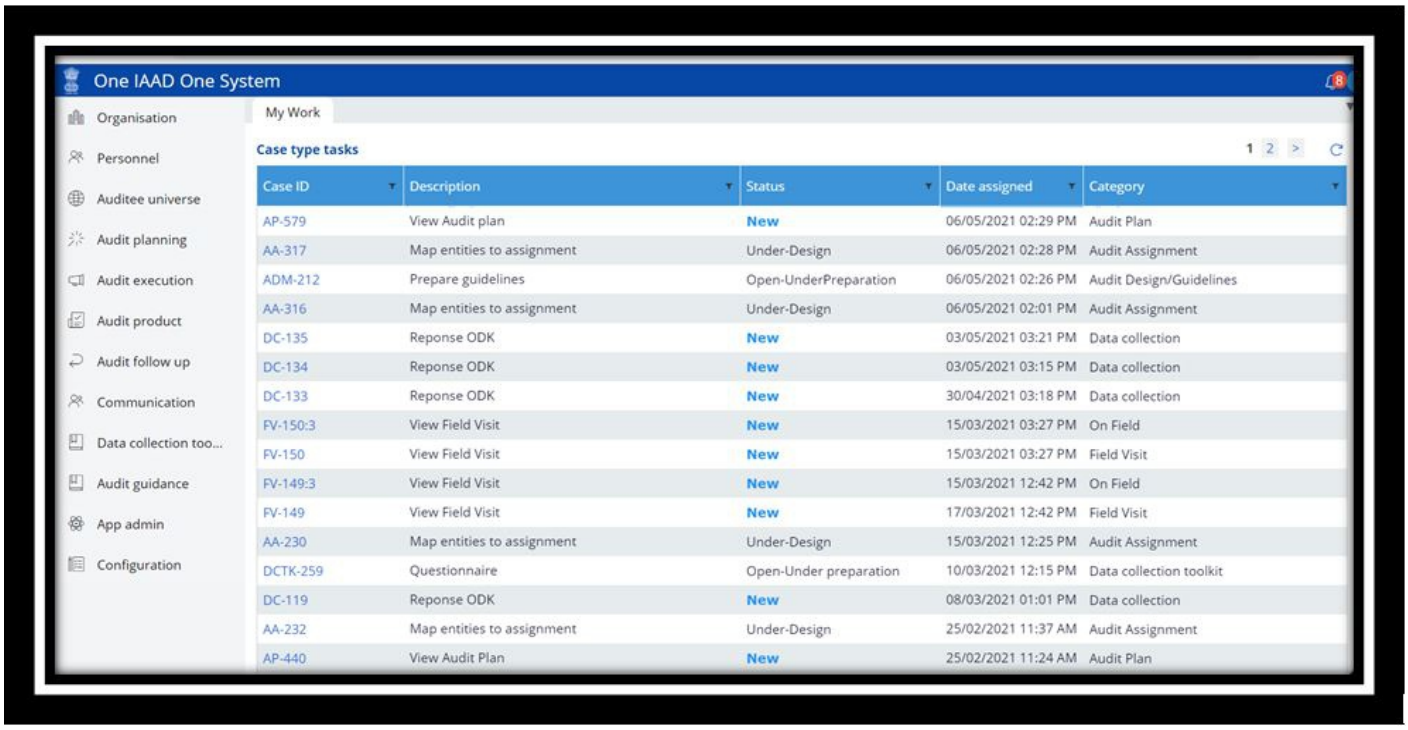
Overview of the OIOS

Sr. No.	Name of Module	Objectives of Module
1	Organization	• List of offices/branch offices and their reporting relationship. • Internal Hierarchy in each offices/branch offices along with the Post hierarchy. • Internal office structure of audit offices. • Roles Master is the bundle of privilege • In Privilege Master we saw what all the privilege given under various modules.
2	Personnel	• Master list of all the employees along with basic information • Data related to their posting/transfer/additional charges • Gradation list (Upcoming phase) • Manage processes for leave, tour, medical claim.
3	Audit Universe	• Master list of Auditee Entity with their Hierarchy. • Basic Information of auditee
4	Audit Planning	• Preparation of Annual Audit Plan • Audit Assignment with mapping of auditable entities. • Review Progress against audit plans
5	Audit Design	• Creation of Audit Design Matrix • Methodology adopted in sampling approach for the selection of Audit entity. • Linkage of Data toolkit Collection
6	Audit Execution	• Composition of Audit team party • Preparation of Audit programme • Initiation of field visit, issue record requisition, audit enquiry, and audit observation • Attachment of key documents, documentation of entry and exit conference. • Receive the responses on audit enquiry/observations from the auditee.
7	Audit Reporting	• Preparation of audit product like IR, SOF, DP, DAN, ML, CAG Audit Report and various Audit certificate for attention of financial attest audit. • Mark and link the KD in the draft. • Add recommendation to report.
8	Audit Follow up	• Follow up of observation in selected audit products • Maintaining information regarding external follow up like PAC/CoPU
9	Data Collection Toolkit	• Collection of data on adhoc/assignment driven for various purpose for example survey conducted by CAG on various topic, beneficiary surveys as a part of Performance audit. • Help in taking collective responses, decision making.
10	Communication	• Functioning of DAK in OIOS • Receipt inward communication • Dispatch outward communication
11	ITA/PR/IW	• Inspection of internal test audit and follow up of internal test audit observation • Planning and Execution of peer review for the field audit offices. • Carry out Inspections by Inspection Wing in C&AG headquarters
12	Knowledge Management System (KMS)	• Document and records related to audit guidance • Uploading of file, order, act, etc in audit information system for audit team. • KMS can be used for keeping the data (ADM, Data Collection Toolkit) in central repository server.

संकाय स्तंभ (FACULTY COLUMN)

Overview of the OIOS

Sr. No.	Name of Module	Objectives of Module
13	Reporting/ Business Intelligence (BI)	• Help in creation of MIS reports. • Creation of Dashboards for controlling
14	Technical Guidance and Support (TGS)	• Provide TGS for audit by Examiner/ local Fund Accounts of PRI and ULBs
15	Administration (Non- HR)	• Procurement Process • Maintaining the records of Inventory and assets (Movable/ Non-movable) • Complaints and request information under RTI Act.
16	Data Migration	• Provide service for bulk data migration • Data entry through prescribed web forms.



Conclusion

Further, Success of any project is reflected by the achievement of expected outcome. The valuable feedback is our baseline to measure and establish a benchmark from which to compare results over time.